UAH

DATOS PERSONALES: PASADO, PRESENTE Y FUTURO DE SU PROTECCIÓN FRENTE A LA COVID-19

PERSONAL DATA: PAST, PRESENT AND FUTURE OF ITS PROTECTION AGAINST COVID-19

Máster Universitario en Acceso a la Profesión de Abogado

Presentado por:

D. JUAN OLMEDILLA HERNÁNDEZ

Dirigido por:

D. CARLOS BALLESTEROS MUÑOZ

Co-dirigido por:

Dª. MÓNICA ARENAS RAMIRO

Alcalá de Henares, a 16 de abril de 2021

D. Carlos Ballesteros Muñoz

CERTIFICA:

Que el trabajo titulado: “DATOS PERSONALES: PASADO, PRESENTE Y FUTURO DE SU PROTECCIÓN FRENTE AL COVID-19”, ha sido realizado bajo mi dirección por el alumno D. Juan Olmedilla Hernández.

Alcalá de Henares, a 16 de abril de 2021

Firmado:

ÍNDICE

PRESENTACIÓN

1. RESUMEN

Este Trabajo Fin de Máster plantea el conflicto que existe entre algunas medidas frente a la COVID-19 y los derechos a la protección de datos y a la intimidad. Para este fin se presenta, en primer lugar, el pasado de ambos derechos para que comprendamos mejor el marco regulador actual, que también se explica.

Una vez superado aquel apartado, se describirán las medidas que se han tomado frente al coronavirus que presentan dudas en lo relativo a la protección de datos y derecho a la intimidad.

En último lugar se pretende hacer dos pequeñas aportaciones al ya laborioso trabajo que desempeñan quienes trabajan a diario por contener la pandemia.

2. ABSTRACT

This paper raises the conflict that exists between some measures against COVID-19 and privacy rights, as well as data protection. For this purpose, the past of both rights is presented in order to understand better the current regulatory framework, which is also explained.

Once that section has been passed, measures that have been taken against the coronavirus that present doubts regarding data protection and the right to privacy will be described.

Finally, it is intended to make two small contributions to the already laborious work done by those who work every day to contain the pandemic.

3. PALABRAS CLAVE / KEY WORDS

Derecho a la privacidad, derecho a la intimidad / Right to privacy

Protección de datos / Data protección

COVID – 19

Coronavirus

4. LISTA DE ABREVIATURAS

AEPD	Agencia Española de Protección de Datos
API	Application Programming Interface
ARCO	Acceso, Rectificación, Cancelación, Oposición
CE	Constitución Española
CEDH	Convenio Europeo de Derechos Humanos, hecho en Roma el 4 de noviembre de 1950
COVID	Coronavirus Desease
CP	Código Penal
LO	Ley Orgánica
LOPDGDD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
LORTAD	Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de carácter personal.
RGPD	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
TC	Tribunal Constitucional
TEDH	Tribunal Europeo de Derechos Humanos
TJUE	Tribunal de Justicia de la Unión Europea
UE	Unión Europea
VIH	Virus de Inmunodeficiencia Humana

5. INTRODUCCIÓN

Estamos en el mejor y, a la vez, peor momento para el derecho a la intimidad y la protección de datos: por un lado, tenemos mayor capacidad para conocer y controlar los datos personales que facilitamos; por otro, es imposible hacer nada en internet sin dejar un mínimo rastro, y eso sólo en el mejor de los casos porque, normalmente, prácticamente cedemos nuestra alma cuando descargamos una aplicación.

En este contexto nos hemos visto envueltos en una pandemia que ha dejado del revés al mundo. Para revertir la situación, todos los estamentos sociales, económicos y políticos hacen todo lo que está en su mano.

Se suele decir que, a grandes males, grandes remedios, y se han tomado medidas extremas como encerrar millones de personas en sus casas. No se cuestiona para nada la efectividad de las medidas ni la necesidad. Lo que se muestra en las próximas páginas es qué tensiones jurídicas plantean las medidas tomadas y qué alternativas se pueden adoptar.

Antes de empezar, es necesario explicar que no es lo mismo el derecho a la intimidad que el derecho a la privacidad. Desde el punto de vista filosófico, las actitudes íntimas son aquellas que no son observadas ni pueden ser observables, tales como pensar o sentir[1]; mientras que el derecho a la intimidad es aquello que encontramos en la Declaración Universal de Derechos del Hombre, el Convenio Europeo para la protección de los Derechos Humanos y de las Libertades Fundamentales y el artículo 18 CE, es decir "*la intimidad es un ámbito o reducto en el que se veda que otros penetren*[2]".

La actitud privada sería aquella que podría ser observable, pero el sujeto que quiere actuar privadamente pone barreras para no ser observado[3], como cuando se baja la persiana de una ventana que da a la calle para que los transeúntes no ven el interior.

Por otro lado, está el derecho a la privacidad, que apareció por primera vez en Estados Unidos en un artículo jurídico en 1890, y se definió como "*the right to be let alone*", es decir, "el derecho a que me dejen estar solo"[4]. Se trataba de que la

---

[1] CASTILLA DEL PINO, C., 1989. Público, privado, íntimo. In: De la intimidad. Crítica. *Público, Privado, Íntimo*. PP. 25-31.
[2] SENTENCIA 73/1982, de 2 de diciembre del Tribunal Constitucional
[3] CASTILLA DEL PINO, C., Op.cit. PP. 25-31.
[4] SALGADO SEGUIN, V. *Intimidad, privacidad y honor en Internet* . Disponible en: https://telos.fundaciontelefonica.com/archivo/numero085/intimidad-privacidad-y-honor-en-internet/.

Administración y el resto de los poderes públicos no se entrometiesen en la vida personal de uno sin su consentimiento o autorización judicial.

Aunque en España el ciudadano de a pie ha equiparado *intimidad* y *privacidad* en la práctica, no hace tantos años se evitaba el segundo término. Por un lado, la RAE no incorporó la palabra a su diccionario hasta 2001[5]; y las diferentes guías de estilo de aquella época recomendaban otras palabras como *intimidad* o *vida privada*[6].

Y aun haciendo un uso indistinto en el español, *privacidad* en realidad tiene su propio significado. La privacidad supone una esfera una esfera mayor que la intimidad pues incluye todos los datos relativos a una persona que deben ser protegidos frente a la injerencia de terceros, sean éstos íntimos o no[7].

En este sentido apunta la importante Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, en su Fundamento Jurídico 6:

"La función del derecho fundamental a la intimidad del art. 18.1 CE es la de **proteger** frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio, FJ 8). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un **poder de control** sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, por esta razón, y así lo ha dicho este Tribunal (SSTC 134/1999, de 15 de julio, FJ 5; 144/1999, FJ 8; 98/2000, de 10 de abril, FJ 5; 115/2000, de 10 de mayo, FJ 4), es decir, el poder de resguardar su vida privada de una publicidad no querida. […]

De ahí la singularidad del derecho a la protección de datos, pues, por un lado, su objeto es más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que

[5] Íbid.
[6] DÍAZ ROJO, J.A. *Privacidad.* Disponible en: https://webs.ucm.es/info/especulo/cajetin/privacid.html.
[7] SALGADO SEGUIN, V. Op.cit..

pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal (STC 170/1987, de 30 de octubre, FJ 4), como el derecho al honor, citado expresamente en el art. 18.4 CE, e igualmente, en expresión bien amplia del propio art. 18.4 CE, al pleno ejercicio de los derechos de la persona. El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado.

De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal".

Resulta que el Tribunal Constitucional reveló hace veinte años la naturaleza de ambos conceptos: el derecho fundamental a la intimidad **protege** la injerencia en la vida personal y familiar, es decir, se trata de un derecho negativo; sin embargo, el derecho -también- fundamental de la protección de datos otorga **control** al individuo sobre sus datos personales, lo que requiere una posición activa. Es por esto por lo que el Reglamento General de Protección de Datos nos ofrece los derechos de acceso, rectificación, oposición y supresión, porque es necesario que la persona interesada tenga una actitud proactiva.

6. OBJETIVOS

Los objetivos son:

- Observar la historia, evolución y regulación de los derechos a la privacidad e intimidad a lo largo de los años.
- Explicar qué medidas frente a la COVID-19 se están tomando que entran en colisión con los derechos a la privacidad e intimidad.
- Proponer una solución realista a los problemas descritos a lo largo del texto.

7. PLAN DE TRABAJO

Para el primer objetivo se atiende al marco regulatorio y jurisprudencial del derecho a la privacidad en Europa desde sus inicios hasta la actualidad. También se estudian otros terceros países, en particular Estados Unidos y los conflictos que ha supuesto forma de entender y tratar datos personales

Para el segundo objetivo se recopilan las medidas adoptadas para frenar la expansión de la pandemia que han podido suponer una limitación de los derechos a la privacidad e intimidad. Lo descrito sobre estas acciones está actualizado a la fecha de presentación de este trabajo, aunque se advierte que los datos e información aportada pueden cambiar próximamente pues es un apartado que está muy pegado a la actualidad.

Finalmente, se presentan dos humildes ideas para tratar algunos de los problemas expuestos en el trabajo, y en particular, sobre lo desarrollado sobre rastreadores, su autoridad y la búsqueda de contactos estrechos de personas infectadas.

I. EL MARCO REGULATORIO DE LA PROTECCIÓN DE DATOS

1. EVOLUCIÓN DE LA REGULACIÓN Y JURISPRUDENCIA SOBRE LA PROTECCIÓN DE DATOS EN EUROPA Y ESPAÑA

1.1 Precursores internacionales

Antes de desarrollar lo que reza el título del presente apartado, cabe hacer una mención especial al que fue de las primeras declaraciones internacionales significativas sobre el derecho a la intimidad[8]: el artículo 5 de la Declaración Americana de Derechos y Deberes del Hombre[9], que decía que "toda persona tiene derecho a la protección de la ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar", seguido del derecho a la inviolabilidad del domicilio[10] y de la correspondencia, así como su libre circulación[11]. Llama la atención que la expresión "vida privada y familiar" es el nombre exacto de un artículo del CEDH, como se verá más adelante.

Meses después se presentó la Declaración Universal de Derechos del Hombre[12]. Su artículo 12 decía -y dice-: "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o reputación. Toda persona tiene el derecho a la protección de la ley contra tales ataques e injerencias". Han pasado más de setenta años desde la redacción de este artículo y, si bien no cabe duda de que es un precepto contundente, hoy en día casi suena a brindis al sol.

A continuación, se procederá a hacer un recorrido por la evolución de la protección de datos en Europa y España a través de su regulación y jurisprudencia.

1.2 Primeros pasos en Europa

1.2.1 Convenio para la protección de los derechos y de las libertades fundamentales, hecho en roma el 4 de noviembre de 1950

Alemania, Italia y el resto de los Estados democráticos de Europa encontraron en la Segunda Guerra Mundial un motivo para constituir sistemas internos constitucionales

---

[8] REBOLLO DELGADO, L. y SALTOR, C.E., 2015. El derecho a la protección de datos en España y Argentina : orígenes y regulación vigente. Madrid: Dykinson. P. 34.

[9] Aprobada como recomendación por la IX Conferencia Interamericana, del 30 de marzo al 2 de mayo de 1948, en Bogotá

[10] Art. 9 de la Declaración Americana de Derechos y Deberes del Hombre de 1948

[11] Art. 10 de la Declaración Americana de Derechos y Deberes del Hombre de 1948

[12] Proclamada por la Asamblea General de Naciones Unidas, resolución 217 A (III), 10 de diciembre de 1948

y supranacionales de control para que la historia no se repitiera[13]. Siguiendo la estela de las Naciones Unidas se crea, entre otras cosas, el Consejo de Europa y el Convenio para la protección de los derechos y de las libertades fundamentales, el cual también instituye en su artículo 19 el Tribunal Europeo de Derechos Humanos. Para permanecer en las diversas organizaciones internacionales, es imprescindible que los Estados candidatos respeten las libertades de sus ciudadanos[14]. Para concretar este requisito, el Consejo de Europa elabora varios Tratados con el paso de los años, empezando por el Convenio de Roma de 1950 que nos ocupa.

El TEDH clasifica los derechos del Convenio en tres tipos: inderogables, donde no caben restricciones; mínimos y configurables, pero respetando los requisitos mínimos del Convenio; y aquellos que son objeto de limitación, cuyos artículos tienen la misma estructura compuesta por un primer párrafo en el que se describe el derecho, y un segundo párrafo en el que se indica cómo pueden los Estados restringir el derecho[15]. El derecho a la vida privada y familiar del artículo 8 se encuentra en este último grupo, y dice lo siguiente:

"*Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia*".

No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".

Destaca en el punto segundo, en lo que concierne al presente TFM, la mención a la "protección de la salud". En cualquier caso, cabe recordar que, si bien este Convenio presenta los requisitos mínimos para los Estados miembros, el artículo 35 de la misma norma obliga a agotar las vías de recurso internas para poder pedir amparo al TEDH.

---

[13] RODRÍGUEZ DÍAZ, B. (Coordinadora), RAMOS DE MOLINS, A. y SANZ GANDASEGUI, F., 2015. Manual de ámbito jurisdiccional comunitario e internacional. Guía práctica para abogados ante la UE y el TEDH. Dykinson. P. 91.
[14] Íbid, P. 92
[15] Íbid, P. 93

La jurisprudencia del TEDH ha demostrado a lo largo de los años que el derecho a la vida privada y familiar no es estanco, que está relacionado con otros derechos del Convenio como se puede ver en el Anexo 1[16]: derecho a la vida; prohibición de la tortura; derecho a un juicio justo; libertad de pensamiento, de conciencia y religiosa; libertad de expresión; derecho a un recurso efectivo; prohibición de discriminación; demandas individuales; protección de la propiedad; y libertad de movimiento.

1.2.2. Convenio 108 del Consejo de Europa, de 28-1-1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981.

Se trata del primer instrumento internacional jurídicamente vinculante sobre la protección de datos[17], y están adheridos a él Suecia (desde 1982), Francia (1983), España (1984), Noruega (1984) y Alemania (1985). Su propósito es "*garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona ("protección de datos")*"[18] . No se debe subestimar este Convenio por tratarse en el apartado de los primeros pasos de la protección de datos en Europa, pues presenta conceptos que, además de estar vigentes, son clave para la materia.

En el artículo 2, apartado a) se introduce el concepto de "datos de carácter personal", que son aquellos relativos a una persona física identificada e identificable. También se define en este artículo "fichero automatizado", como aquel conjunto de informaciones que son objeto de un tratamiento automatizado; "tratamiento automatizado", como operaciones realizadas con ayuda de procedimientos automatizados; y autoridad "controladora del fichero", como la persona física o jurídica

[16] European Court of Human Rights. 2020. Guide on Article 8 of the European Convention on Human Rights. Right to respect for private and family life, home and correspondence. PP. 13-20. Tabla del Anexo de elaboración propia.

[17] MARZOCCHI, O., 2020. *La protección de dos datos personales.* Diciembre. Disponible en: https://www.europarl.europa.eu/factsheets/es/sheet/157/la-proteccion-de-los-datos-personales#:~:text=El%20Convenio%20n.,de%20la%20protecci%C3%B3n%20de%20datos.

[18] Art. 1 del Convenio 108 del Consejo de Europa, de 28 de enero de 1981

responsable de decidir cuál será la finalidad del fichero, qué categorías de datos se establecen, y qué operaciones se aplicarán.

Más adelante se presentan los principios básicos para la protección de datos: compromiso de las Partes para la aplicación de los preceptos[19]; criterios de calidad de los datos[20]; establecimiento de categorías particulares de datos, que sólo se podrán tratar automáticamente si el derecho interno prevé garantías adecuadas[21]; seguridad de los datos frente a su pérdida o destrucción accidental o no autorizada, así como el acceso, la modificación o difusión no autorizados[22].

El artículo 8 es el precursor de lo que más tarde se conocerá como derechos ARCO[23], que serán objeto de estudio más adelante. Sin ánimo de realizar una enumeración exhaustiva, este artículo establece que cualquier persona debe: a) poder conocer la existencia de un fichero automatizado de datos personales y sus características; b) obtener información de la existencia de ficheros automatizados que conciernen a la persona; c) rectificar o borrar los datos cuando se infrinjan las disposiciones del derecho interno o del presente Convenio; d) disponer de un recurso si no se ha atendido a lo previsto en los puntos b) y c).

Se puede exceptuar lo previsto en los artículos 5, 6 y 8 en favor de la seguridad pública, entre otros motivos; así como los puntos b), c) y d) del artículo 8 con fines estadísticos o científicos cuando no existan riesgos manifiestos que atenten contra la vida privada24.

En cuanto a las disposiciones relativas a las relaciones entre Estados, el artículo 12 indica que un país no podrá prohibir el flujo de datos personales a otro Estado alegando sólo la protección de la vida privada, salvo que los datos en cuestión requieran una reglamentación particular y la otra parte no tenga una protección equivalente; así como en el caso de que el Estado no sea parte del Convenio. Además, el artículo 13 exige cooperación entre los Estados parte del Convenio.

---

[19] Ibíd. Art. 4.
[20] Ibíd. Art. 5: los datos se obtendrán legal y legítimamente; con finalidades determinadas y legítimas; serán adecuados, pertinentes y no excesivos para el propósito buscado; serán exactos y actualizados; y se conservarán por un tiempo limitado, de modo que se permita la identificación de las personas concernidas.
[21] Ibíd. Art. 6: origen racial; opiniones políticas; convicciones religiosas u otras convicciones; salud; vida sexual; y condenas penales.
[22] Ibíd. Art. 7.
[23] Acceso, Rectificación, Cancelación, Oposición.
[24] Íbid, Art. 9.

El 28 de enero de 2021, España ratificó la actualización del Convenio, denominado como "108+". Dicha versión entrará en vigor cuando todos los Estados ratifiquen el convenio, o el 11 de octubre de 2023 cuando lo hayan hecho 38 países. A 29 de marzo de 2021 lo han ratificado 11 partes[25]

1.3 Algunas Sentencias relevantes del Tribunal Europeo de Derechos Humanos

1.3.1 Caso de Malone v. Reino Unido (Sentencia 8691/79), de 2 de agosto de 1984: registro de contactos

James Malone fue acusado en 1977 de un delito de receptación. En el transcurso del juicio se descubrió que su teléfono fue intervenido anteriormente con la autorización del Ministro del Interior. En 1979, al no haberse vistas satisfechas sus pretensiones, Malone acude al TEDH alegando la vulneración de los artículos 8 y 13 del Convenio Europeo de Derechos Humanos, sobre el derecho al respeto a la vida privada, familiar, y el secreto de las comunicaciones y correspondencia; así como al derecho a un recurso efectivo; afirmó que se habían intervenido sus comunicaciones telefónicas y por correspondencia, y que se grabaron los números con los que contactaba.

Lo cierto es que el artículo 58.1 la Ley de 1953 sobre el Post Office, la compañía de mensajería por el que pasaba la correspondencia, preveía la interceptación de las comunicaciones "en cumplimiento de una orden expresa firmada por un Ministro". Este precepto también se aplicaba a las conversaciones telefónicas, pues ya se consideraba "comunicación telegráfica" en una sentencia de 1880[26], y el artículo se aplicaba al telégrafo, que se categoriza como "objeto postal" en el artículo 87.1 de la Ley.

Sobre la justificación de las interceptaciones, el TEDH recuerda que el artículo 8.2 del CEDH señala que la injerencia en las comunicaciones debe estar "prevista en la ley"[27], que debe ser asequible para el ciudadano y expresada con la suficiente precisión como para que exista seguridad jurídica[28]. También se requiere un mínimo de calidad a la ley, en el sentido de que el Derecho interno debe ofrecer protección frente a posibles

---

[25] Chart of Signatures and Ratifications of Treaty 223. Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. 29 de marzo de 2021. Disponible en: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures.
[26] Attorney General v. Edison Telephone Company, QueenŽs Bench Division, volumen 6, 1880, P. 244
[27] Apartado 66, Sentencia 8691/79.
[28] Sentencia en el caso Sunday Times, pág. 31, apartado 49; sentencia en el caso Silver y otros, P. 33, apartados 87 y 88.

vulneraciones arbitrarias de la Administración[29]. Además, si la ley proporciona a las autoridades una facultad discrecional, también debe fijar su alcance.

Atendiendo ahora al caso concreto, el Derecho inglés y galés no preveía la intromisión con exactitud[30], no se determinaba con suficiente claridad el alcance de la discrecionalidad de la medida. Un sistema de interceptación de comunicaciones puede ser necesaria y compatible con el artículo 8.2 del Convenio, pero estas escuchas no estaban previstas con todas las garantías en la ley.

El otro pilar del conflicto se encuentra en el "recuento". Se trata de un dispositivo que, por aquel entonces, registraba los números marcados por un teléfono, la hora y la duración de la llamada. Se utilizó en el caso concreto para saber con quién había contactado Malone, y luego los contactos soportaron registros domiciliarios. Fuera de esto, el Post Office lo utilizaba para asegurar el servicio de teléfono y, si bien no interceptaba las comunicaciones, podría suponer problemas en relación con el artículo 8. De hecho, el Tribunal entiende que también vulnera el artículo 8 por los mismos motivos que se explicaron en el párrafo anterior.

Este último punto, el del registro de los contactos, es relevante para el control de la propagación del COVID-19. Las motivaciones y finalidades en ambos casos son muy diferentes, no cabe duda, pero tampoco está claro en qué normativa se sustenta la guía para la identificación y seguimiento de contactos de casos de COVID-19[31].

1.3.2 Caso de Leander v. Suecia (Sentencia 9248/81), de 26 de marzo de 1987: el interés general

Leander accedió a un trabajo temporal como carpintero por un periodo determinado a un museo naval que se encontraba junto a una base -también- naval, el 20 de agosto de 1979. Aunque el trabajo iba a tener una duración de diez meses, el trabajador fue despedido el 3 de septiembre del mismo año como resultado de un control derivado de la Orden de Control de Personal de 1969. El motivo detrás de esta medida era que el trabajo que desempeñaba Leander requería poder tener acceso a la base naval y, en favor

[29] Apartado 67, Sentencia 8691/79.
[30] Apartado 79, Sentencia 8691/79.
[31] Ministerio de Sanidad de España. *Documentos Técnicos Para Profesionales.* Disponible en: https://www.mscbs.gob.es/profesionales/saludPublica/ccayes/alertasActual/nCov-China/documentos.htm.

de la seguridad nacional, se consideró que el trabajador contaba con unos antecedentes que hacían peligrar esa seguridad. Le dijeron que podría optar a otro trabajo que no requiriese esa capacidad, pero no podía continuar en este puesto.

Leander quiso saber con qué información contaban las autoridades para llegar a semejante conclusión, pero no se le dio respuesta. El afectado afirma no haber cometido delito alguno, que lo peor que ha hecho fue llegar tarde a un desfile durante el servicio militar; y añade también, sugiriendo motivos políticos, que fue miembro del Partido Comunista de Suecia. Leander no cuestiona la finalidad de la norma -protección de la seguridad nacional y en detrimento de la vida privada-, sino que él haya hecho algo que se corresponda con el hecho que ésta prevé.

El TEDH desestimó las pretensiones del demandante, pues entendió que la injerencia estaba debidamente prevista en la Ordenanza, además de ser ésta fácilmente accesible sin mayores dificultades por parte del perjudicado, por lo que la medida cumplía con los requisitos necesarios[32]. Además, los controles secretos tenían relación directa con la seguridad nacional, por lo que no se le debe equiparar con otras actuaciones ordinarias en las que se debe atender a la previsibilidad y no discriminación de trato[33].

Finalmente, continúa el Tribunal explicando que la injerencia se corresponde con una necesidad social imperativa y proporcional al fin legítimo que se persigue, todo ello contando con unas estrictas garantías, cosa que se cumplía en este caso[34].

Aunque la intención era llevar a cabo un relato cronológico de la jurisprudencia y normativa, para pasar del derecho de la vida privada a los datos de salud hay que dar un salto en el tiempo.

1.3.3 Caso de I v. Finlandia (Sentencia 20511/03), de 17 de julio de 2008: los datos de salud

La recurrente trabajó como enfermero en un hospital entre 1989 y 1994. Este hombre comenzó a realizar visitas al policlínico de enfermedades infecciosas del mismo centro, con diagnóstico de VIH positivo. A principios de 1992 sus compañeros empezaron

---

[32] CASTRO-RIAL GARRONE, F., 1987. Decisiones de la Comisión y del Tribunal Europeos De Derechos Humanos. Revista de Instituciones Europeas, no. 15. P. 909.
[33] Íbid.
[34] Íbid, P. 910.

a sospechar de su estado de salud pues, por aquel entonces, el personal del hospital tenía libre acceso al historial clínico de los pacientes. Tras haberle comentado esto a su doctor en verano de ese año, se modificaron las condiciones de acceso a los historiales. I. usaba un nombre falso, pero se le cambió después, así como se le asignó un nuevo número de seguridad social.

En 1995 no pudo continuar en su puesto de trabajo al no renovarse su contrato temporal, y en noviembre de 1996 solicitó el registro de las personas que habían accedido a sus datos personales, sin éxito.

Así, la recurrente termina por llegar hasta el TEDH alegando la vulneración del artículo 8 del Convenio, por la falta de diligencia de las autoridades sanitarias a la hora de establecer un registro sobre las personas que acceden datos confidenciales. Y lo que dice el TEDH en este sentido es importante: la obligación del artículo 8 no es una mera protección de las personas frente a las inferencias de la administración pública, sino que también es un mandato que genera obligaciones para así brindar una protección efectiva de la vida privada. Esto es, no se trata solamente de no inmiscuirse en lo privado, sino desarrollar una actividad real y efectiva para hacer efectivo este derecho.

1.4 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

La libre circulación de datos tiene relación directa con la de bienes y servicios y, con el fin de armonizar las leyes nacionales de los Estados miembros de la por aquel entonces Comunidad Europea, se adoptó esta Directiva en 1995[35].

La Directiva continuó el camino andado por las leyes nacionales y el Convenio 108, pues los conceptos principales eran prácticamente iguales; pero también mejoró algunos aspectos. Por ejemplo, se aprovechó el artículo 11 del Convenio 108, sobre la posibilidad de establecer una protección más amplia[36], para introducir en la norma un

[35] Agencia de los Derechos Fundamentales de la Unión Europea; Consejo de Europa; Tribunal Europeo de Derechos Humanos; Buttarelli, G. 2018. Manual de legislación europea en materia de protección de datos., p. 33.

[36] "Ninguna de las disposiciones del presente capítulo se interpretará en el sentido de que limite la facultad, o afecte de alguna otra forma a la facultad de cada Parte, de conceder a las personas concernidas una protección más amplia que la prevista en el presente Convenio".

control independiente para así hacer efectivo el cumplimiento de la Directiva[37]. Tanto es así que el Consejo de Europa tomó nota y en 2001 incorporó esta idea al Convenio 108 a través del Protocolo adicional.

Otra novedad que trajo consigo la Directiva fue ampliar el ámbito de aplicación, llegando así hasta los ficheros manuales y no sólo los automáticos[38]; y se excluye expresamente los datos de personas físicas en la esfera personal y doméstica, seguridad y defensa, etc. También recogen las técnicas para procesar los datos personales compuestos por imagen y sonido. Ahora bien, cabe detenerse en el Capítulo IV, pues tiene mucha relación con los -entonces- futuros quebraderos de cabeza con Estados Unidos: la transferencia de datos personales a terceros países.

El artículo 25 de la Directiva decía que se permitía a los Estados miembro la transferencia de datos personales con un tercer Estado cuando éste garantice un nivel de seguridad "adecuado", para lo que "*se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países*". El artículo 26 completaba este breve Capítulo con una lista de excepciones cuando no se garantice un mínimo nivel de protección: que el interesado haya dado su consentimiento inequívocamente a la transferencia prevista; o que la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado; o que la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero; o que la transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial; o que la transferencia sea necesaria para la salvaguardia del interés vital del interesado; o la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté

[37] Íbid, P. 33.
[38] MAYOR GÓMEZ, R., 2016. Contenido y novedades del Reglamento General de Protección de Datos de la UE (Reglamento UE 2016/679, de 27 de abril de 2016). Revista del Gabinete Jurídico de la Junta de Comunidades de Castilla-La Mancha, no. 6. P. 3.

abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta. También se admite "*cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos*".

Esta norma supuso un importante avance que materializaba sobre el papel el interés de los Estados miembros por actualizarse en la materia, pero quizá la Directiva no era la mejor herramienta para armonizar los diferentes ordenamientos jurídicos.

El artículo 288 del Tratado de Funcionamiento de la Unión Europea (antes, 249 del Tratado Constitutivo de la Comunidad Europea) establece cuatro herramientas para ejercer las competencias de la Unión, de las cuales nos detendremos sólo en las dos primeras: reglamento, que "*tendrá un alcance general. Será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro*"; y directiva, que "*obligará al Estado miembro destinatario en cuanto al resultado que deba conseguirse, dejando, sin embargo, a las autoridades nacionales la elección de la forma y de los medios*". Por tanto, ambas herramientas son de obligado cumplimiento, pero la Directiva que nos ocupa sólo obliga en cuanto a objetivos y no en cuanto al cómo se alcanzan.

Esto supuso que cada Estado hiciera su propia interpretación de las normas, definiciones y gravedad de las infracciones; así como se aplicaron diferentes formas de control[39].

1.5 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Afortunadamente, España no agotó el plazo de 12 años que daba la Directiva para transponerla, y en 1999 se incorporó a nuestro ordenamiento jurídico. Como principal diferencia respecto a la LORTAD[40], la predecesora de esta LO, la trasposición incluía menos excepciones -y más razonables- en cuanto al régimen general de aplicación; pero

[39] Íbid, P. 34.
[40] Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. BOE núm. 262, de 31 de octubre de 1992. PP. 37037 a 37045

no alteraba prácticamente nada la lista de excepciones relativas a los derechos de los afectados[41], por lo que en este sentido no se produjo mayor avance.

II. REGULACIÓN ACTUAL DE LA PROTECCIÓN DE DATOS

1. REGLAMENTO (UE) 2016/679, DE 27 DE ABRIL DE 2016, RELATIVO A LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES Y A LA LIBRE CIRCULACIÓN DE ESTOS DATOS Y POR EL QUE SE DEROGA LA DIRECTIVA 95/46/CE (REGLAMENTO GENERAL DE PROTECCIÓN DE DATOA)

El considerando 6 del RGPD resume bastante bien sus propósitos[42]: "La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales".

El primer punto que destacar es el consentimiento y la protección de datos particularmente sensibles. El consentimiento del interesado es "*toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen*" (art. 4.11) RGPD). Dicho consentimiento se puede dar de cualquier manera, incluso con la marcación de casillas en una web[43] -esto se ve siempre que entramos en cualquier página-. Además, si la recogida de información tiene varios

[41] GARRIGA DOMÍNGUEZ, A., 2000. La nueva Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos personales, ¿un cambio de filosofía? Anales de la Cátedra Francisco Suárez, vol. 34. P. 320.
[42] GARCÍA-PERROTE ESCARTÍN, I. y MERCADER UGUINA, J.R., 2017. El Reglamento (UE) 2016/679 Del Parlamento Europeo y del Consejo de 27 de abril relativo al tratamiento de datos personales, un primer acercamiento. Revista de información laboral, no. 2/2017. P. 1.
[43] Íbid P. 2.

fines, se debe dar el consentimiento expreso para cada finalidad. Esta es una de las grandes virtudes del RGPD pues sabemos con precisión qué información damos y para qué. Después está la información particularmente sensible que afecta a derechos fundamentales: ideología, religión y creencias, afiliación sindical, origen racial, vida sexual, salud y, como novedades, datos genéticos -aquellos relativos a las genéticas heredadas que proporcionen información única sobre la fisiología o salud (art. 4.13)- y biométricos -obtenidos por un tratamiento técnico específico y que dan información sobre características físicas, fisiológicas o conductuales de personas cuando dicha información permita su identificación, como las caras y las huellas dactilares (art. 4.14)-.

Estos datos especialmente protegidos quedan blindados por el artículo 9.1, que prohíbe su tratamiento salvo en las situaciones previstas en el apartado 2: a) consentimiento explícito del interesado salvo que se establezca una prohibición en sentido contrario; b) que los datos sean necesarios para el cumplimiento de obligaciones por parte del responsable o del interesado en el ámbito del Derecho laboral y de la seguridad o protección social; c) cuando el tratamiento sea necesario para proteger intereses vitales de una persona física que esté incapacitada para dar su consentimiento; d) cuando el responsable del tratamiento sea una persona jurídica sin ánimo de lucro cuya finalidad sea política, filosófica, religiosa o sindical -se entiende que si uno se afilia a un sindicato, por ejemplo, es imposible que el sindicato no tenga datos de afiliación sindical-; e) cuando los datos los manifestó públicamente el interesado; f) cuando sea necesario el tratamiento para el ejercicio y defensa de reclamaciones, así como por el propio funcionamiento de los tribunales; g) cuando exista interés público esencial y el tratamiento sea proporcional al objetivo perseguido, respetando en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y concretas para proteger los derechos fundamentales del interesado; h) cuando el tratamiento sea necesario con fines de medicina preventiva o laboral; i) cuando sea necesario por razones de interés público en el ámbito de la salud pública; j) o cuando sea necesario con fines de archivo en interés público, investigación científica o histórica o estadísticos. No se trata de una lista de excepciones pequeña, desde luego, pero nos da unos casos concretos que benefician a la seguridad jurídica.

El segundo punto es el de la mejora del principio de la transparencia, esto es, los datos deben ser fácilmente accesibles y sencillos de entender. El principio se aplica en particular en lo concerniente al responsable del tratamiento y la finalidad y tratamientos

de los datos[44]. Los datos que éstos traten deben ser adecuados, pertinentes y limitados a lo necesario para los fines buscados; y para que los datos no se almacenen más tiempo del necesario, el responsable debe establecer plazos su eliminación o revisión periódica. También debe asegurarse de que se toman todas las medidas de seguridad necesarias para garantizar la confidencialidad de los datos y que no sufran accesos no autorizados.

Se incluye en el RGPD el "derecho al olvido", que no deja de ser el derecho de cancelación o supresión que ya existía -más adelante se entrará en el detalle-, pero se le llama así porque se suele emplear en casos en los que el afectado ve su nombre en buscadores de internet de modo que cualquiera puede identificarle con algún acontecimiento pasado, normalmente desagradable, que el individuo quiere que sea olvidado[45]. Otro derecho novedoso es el de portabilidad, que permite al interesado obtener sus datos en un formato que le permita trasladarlos a otro responsable, pudiendo hacerlo incluso del antiguo responsable al nuevo directamente si fuese técnicamente posible.

En tercer lugar, los obligados deben establecer un sistema de control de riesgos en relación con los datos personales. Este sistema debe tener en cuenta la privacidad y protección de los datos en todo el tratamiento de los datos -redes de comunicación, procesos productivos y de negocio-; y se requiere una responsabilidad proactiva del obligado que demuestre que se trabaja de acuerdo con el RGPD, de modo que se tenga en cuenta la privacidad de los datos a la hora de diseñar procedimientos, productos y servicios, así como que por defecto sólo se traten los datos mínimos imprescindibles[46]. El responsable deberá llevar un registro de los tratamientos de datos que se lleven a cabo. Estas obligaciones se aplican en empresas con 250 personas o más; también a las que tengan menos empleados pero que trabajen con datos sensibles (salud, religión, etc.) o relativos a infracciones penales del art. 10 RGPD.

En cuarto lugar, se introducen nuevas formas de control: Privacy Impact Assessments, evaluaciones de impacto, sobre todo cuando exista riesgo para los derechos y libertades. En particular, se aplica en situaciones en las que se maneja muchos datos de una generalidad importante de personas a gran escala, dificultando así a los interesados

---

[44] Íbid, P.2.
[45] Agencia Española de Protección de Datos, 2020. *Derecho de supresión ("al olvido"): Buscadores de internet.* 18 de septiembre. Disponible en: https://www.aepd.es/es/areas-de-actuacion/internet-y-redes-sociales/derecho-al-olvido.
[46] Íbid PP 3-4

el ejercicio de sus derechos[47]. También se crea la figura del Data Protecion Officer, persona nombrada por los organismos públicos -salvo los tribunales- para velar por el cumplimiento del RGPD cuando las actividades que desempeñen impliquen un tratamiento a gran escala de los datos, o cuando se traten de infracciones penales. Un actor similar se pide para empresas, el delegado de protección de datos, cuando se procesen datos a gran escala o cuando éstos pertenezcan a las categorías especiales de datos que mencionábamos antes. Este delegado debe ser designado obligatoriamente en las Administraciones Públicas[48].

Finalmente, se endurecen las sanciones, que ahora pueden alcanzar hasta los veinte millones de euros o un 4% del volumen de negocio del ejercicio financiero anterior, aplicándose el de mayor importe. El artículo 83 establece una lista de elementos a considerar para graduar las sanciones administrativas, las cuales calcula la autoridad de control del Estado -en España, AEPD-. Esos elementos son la gravedad, intencionalidad o negligencia, las medidas tomadas para aminorar los daños, el grado de responsabilidad, antecedentes, las categorías de los datos, la forma en que la autoridad de control tuvo noticia de la infracción -dicho de otro modo, se valora positivamente que el infractor comunique la infracción-, que las medidas del art. 58.2 se hayan ordenado contra el responsable del asunto, que exista adhesión a códigos de conducta del art. 40 o mecanismos de rectificación con arreglo al art. 42, o cualquier otro factor grave o atenuante que se pueda aplicar.

1.1 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Es preciso hacer una aclaración previa: los Reglamentos que proceden de la UE son de directa aplicación, a diferencia de las Directivas, las cuales deben ser traspuestas. El propósito de la LOPDGDD no es trasponer el RGPD, sino complementarlo en aquellos puntos que requieran un poco más de desarrollo.

Un punto que complementa la LOPDGDD es la edad mínima para dar el consentimiento para el tratamiento de datos: el RGPD pone este límite, como regla

[47] Íbid, P.4
[48] Íbid. P 5.

general, en los 16 años, pero permite a los Estados bajar hasta los 13 como máximo, y España ha puesto el mínimo en 14 años. (art. 7 LOPDGDD).

También se añaden en el Título X lo que se han denominado "derechos digitales", donde aparte de mencionar por encima algunas cosas que ya menciona el RGPD derecho al olvido, portabilidad-, también se mencionan lo que suena más a principios rectores que a derechos per se, como el derecho a la neutralidad de internet -proporción de servicios de internet sin incurrir en discriminación por razones técnicas o económicas-, acceso universal a internet, derecho a la seguridad y educación digital, o el de protección de menores en internet.

1.1.1 Derechos del interesado en el ámbito de protección de datos

En los próximos apartados se expone lo que no son otra cosa que las formas en las que se concreta el derecho fundamental a la protección de datos: derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento de los datos y derecho a la portabilidad.

1.1.1.1 Acceso: arts 15 RGPD y 13 LOPGDD

La primera de las acciones posibles es el de acceso a los datos, pedir al responsable confirmación de que efectivamente están siendo objeto de tratamiento, y en caso afirmativo, saber qué datos son[49].

1.1.1.2 Rectificación: arts 16 RGPD y 14 LOPGDD

Una vez que sabemos que están tratando nuestros datos personales podemos solicitar la rectificación de datos inexactos o incompletos, acompañando la petición con documentación que demuestre el error[50].

[49] MERINO MARTÍN, J., 2019. Los datos personales relativos a la salud y la historia clínica. *Revista Aranzadi Doctrinal*, no. 10/2019. PP 7-8.
[50] Íbid. P-8.

1.1.1.3 Supresión: arts 17 RGPD y 15, 93, 94 LOPGDD

La acción de cancelación fue objeto de *rebranding* y se le empezó a llamar derecho de supresión, o incluso "derecho al olvido", pero su propósito no cambia: solicitar la supresión de datos del afectado cuando se de alguna de estas condiciones[51]:

- Los datos no son necesarios para el fin para el que se obtuvieron;
- Que el interesado retire el consentimiento para el tratamiento de los datos de acuerdo con artículo 6, apartado 1, letra a)[52], o el artículo 9, apartado 2, letra a)[53], y este no se base en otro fundamento jurídico;
- Que se oponga al tratamiento de acuerdo con el artículo 21, apartado 1[54], y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2[55].
- Que los datos se hayan tratado ilícitamente.
- Que la supresión responda una obligación legal de la UE o un Estado miembro.
- Que los datos se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1[56] RDPD.

1.1.1.4 Oposición: arts 21 y 22 RGPD y 18 LOPGDD

Como su nombre sugiere, el derecho de oposición consiste en oponerse -valga la redundancia- a que los datos personales sean objeto de tratamiento cuando éste sea necesario para el interés público o en el ejercicio de poderes públicos, o para la

---

[51] Íbid. P-8.

[52] "El interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos".

[53] "El interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado"

[54] "El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones."

[55] "Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia."

[56] "Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó. Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años".

satisfacción de intereses legítimos del responsable del tratamiento, apoyando la oposición en motivos relacionados con la situación personal del individuo[57]. Se parece mucho a la cancelación, pero es diferente: mientras que el derecho a la cancelación se ejercita frente a un tratamiento de datos ilegítimo y/o innecesario, en el caso de la oposición lo que se manifiesta es la voluntad del interesado de que no se siga procesando los datos cuando el motivo de dicho tratamiento sea legítimo o responda al interés general.

1.1.1.5 Limitación del tratamiento: arts 18 RGPD y 16 LOPGDD

Los datos de una persona sólo se tratarán con su consentimiento o porque el procesamiento sea necesario para presentar reclamaciones, para la protección de derechos de terceros o por motivos de interés público[58].

1.1.1.6 Portabilidad: arts 20 RGPD y 17 LOPGDD

El derecho a la portabilidad consiste en la potestad del interesado para recibir los datos personales que el responsable del tratamiento tiene de él[59] y llevarlos a otro responsable de su preferencia, incluso pueden pasar los datos de un responsable a otro si fuese técnicamente posible.

2. LA PROTECCIÓN DE DATOS FUERA DE LA UNIÓN EUROPEA

2.1 Estados Unidos: regulación, del *Safe Harbour* al *Privacy Shield* y el TJUE

La Cuarta Enmienda de la Constitución de los Estados Unidos es lo que más se acerca a una mención a la privacidad, pues no se hace en la norma ninguna mención expresa[60]: "*El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas*". El Tribunal Supremo de EEUU interpreta el literal de la norma como una protección frente a registros de la Administración cuando existe una expectativa de privacidad razonable;

[57] MERINO MARTÍN, J., 2019. Op. Cit.. P. 9.
[58] Íbid, P.8
[59] Íbid, PP.8-9
[60] SUAREZ RUBIO, S.M., 2011. El derecho a la privacidad en el ámbito de la salud: Estados Unidos. Facultad de Ciencias Sociales de Cuenca. P. 5

así como que comprende desde la sexualidad de la persona a la salud, pasando por el control de natalidad, y llegando a la divulgación injustificada de información personal por parte del gobierno[61]. Aparte de esto, luego los Estados sí lo prevén expresamente en sus constituciones, como ocurre en Alaska, Arizona, California, Florida, Hawai, Lousiana, Montana, Carolina del Sur y Washington[62].

Pero la doctrina considera que quienes crearon el concepto de privacidad en EEUU fueron Samuel D. Warren y Louis D. Brandeis con su artículo "*The right to privacy*"[63]. Y sí, fueron ellos quienes acuñaron aquello de "*the right to be let alone*" que se mencionó anteriormente. Después vendría el desarrollo del concepto mediante jurisprudencia, aunque resultaba difícil de seguir porque los casos eran dispersos y difíciles de clasificar, así que Prosser en su *Restament of Torts* presentó cuatro tipos de violación de la intimidad: intrusión en el aislamiento o asuntos de una persona; revelación de hechos vergonzosos; publicidad que muestra una imagen falsa de alguien; y lucro del nombre o apariencia de un tercero[64]. Más adelante, en 1965, el Tribunal Supremo reconoce el derecho a la intimidad como un derecho con sustantividad propia. Se trata de un derecho que, por tanto, ha pasado por muchos años de desarrollo sobre la marcha.

2.1.1 Safe Harbour vs. Schrems

Aquella regulación no era compatible con la Directiva 95/46/CE, pues la UE entendía -y entiende- que la transferencia de datos fuera de la UE debía disponer de una verdadera protección del derecho a la privacidad, así que la Unión y EEUU llegaron a un acuerdo que se materializó en la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América, también conocida como *Safe Harbour*[65]: se trata de una lista de principios a los que pueden acoger las empresas si éstas lo desean, y en tal caso tienen fuerza vinculante. Esta lista se compone

[61] Íbid, P. 6.
[62] Íbid, PP. 6-7.
[63] Íbid, P. 8
[64] Íbid. P. 9.
[65] ORTEGA GIMÉNEZ, A., 2009. Transferencia internacional de datos de carácter personal: UE Vs. EE.UU. Revista de Derecho vLex, no. 67. P.2.

de los siguientes puntos: *notificación*, por el que los obligados por el acuerdo deben notificar a los usuarios de los fines y utilización de sus datos; *opción*, por el que se da a los usuarios el poder de decidir si sus datos se ceden a terceros; *transferencia ulterior*, por el que un tercero que reciba dichos datos deba comprometerse a los dos primeros principios; *seguridad*, por el que las entidades se comprometen a tomar las medidas necesarias para evitar la pérdida, modificación o destrucción de los datos; *integridad de los datos*, por el que los datos deben corresponderse a los fines para los que se toman; *acceso*, por el que los usuarios deben poder conocer qué datos personales tienen sobre ellos y, en su caso, corregirlos, modificarlos o suprimirlos si fueran inexactos; y *aplicación*, por el que los afectados puedan recurrir cuando se vean afectados por el incumplimiento de la normativa de transferencia de datos[66]. El Safe Harbour también recoge una serie de excepciones al cumplimiento del acuerdo: cuando sea en favor de la seguridad nacional, interés público y cumplimiento de la ley; cuando otra ley o resolución jurisdiccional lo establezca; o cuando una norma comunitaria lo permita.

Años después, el por aquel entonces estudiante de Derecho Max Schrems solicitó a Facebook los datos personales que almacenaban de él y recibió un CD con 1.200 -mil doscientas- páginas sobre su actividad en la plataforma[67]. Encontró lo que consideró varias vulneraciones de su privacidad y presentó 22 denuncias, entre otros motivos, por descubrir que Facebook no había borrado conversaciones en su sistema que Max borró en su usuario; o que disponían de los contactos de su agenda cuando la app se sincronizaba, aunque éstos no diesen su consentimiento. Después, en 2013, Edward Snowden hizo su aparición en escena y desveló que la Agencia de Seguridad Nacional de EEUU y el FBI recababan datos personales directamente de los servidores de, por ejemplo, Microsoft, Google o Facebook[68], las cuales se encontraban precisamente entre las más de 4.000 empresas que se adhirieron al Safe Harbour.

Esto fue la vigésima tercera gota que colmaba el vaso de Max, así que tras su poco exitoso paso por la Comisión de Protección de Datos de Irlanda -Facebook tiene su sede europea en este país- junto a sus 22 denuncias, el caso terminó por llegar al TJUE[69], que

---

[66] Íbid, P.3.
[67] ABRIL, G., 2018. *Max Schrems, El Hombre que retó a Mark Zuckerberg.* 18 de mayo. Disponible en: https://elpais.com/elpais/2018/05/10/eps/1525952227_419658.html.
[68] EFE / 20MINUTOS., 2013. *Cronología del 'Caso Snowden', el joven que reveló el espionaje masivo de Estados Unidos.* 7 de julio. Disponible en: https://www.20minutos.es/noticia/1850380/0/caso-snowden/cronologia/espionaje-ee-uu/?autoref=true.
[69] ABRIL, G., 2018. Op. Cit.

declaró inválido el Safe Harbour en su Sentencia de 6 de octubre de 2015 por los siguientes motivos[70]: se estaban conservando la generalidad de los datos sin diferenciarlos en función de su propósito; por el acceso generalizado e indiscriminado de las autoridades públicas a las comunicaciones electrónicas, lo que vulnera el derecho fundamental al respeto a la vida privada -art. 8 CEDH-; y porque no se prevé que el usuario ejerza acciones legales para acceder a sus datos para rectificarlos o suprimirlos, afectando al derecho fundamental a la tutela judicial efectiva -art. 47 CEDH-.

2.1.2 Privacy Shield vs. Schrems II

Viviane Reding, antigua comisaria de Justicia y promotora del actual RGPD[71], confesó que el caso Schrems le hizo pensar que no se podía continuar así[72], y en julio de 2016 nace la Decisión de Ejecución (UE) 2016/1250 de la Comisión de 12 de julio de 2016 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE.UU, también conocido como *Privacy Shield*. El escudo se parece mucho al puerto, pero con pequeñas diferencias[73]: obligaciones más rigurosas para las empresas que tratan con datos personales; mayor claridad y transparencia sobre las injerencias se las administraciones públicas estadounidenses; se dan vías de recurso a los ciudadanos afectados, entre los que está la figura del Defensor del Pueblo que vela por los europeos; y el establecimiento de revisión conjunta anual del Privacy Shield. Sin embargo, como ya ocurrió anteriormente, el escudo fracasó porque no se garantizaba el principio de proporcionalidad de las injerencias en la intimidad de las personas[74]. Se continuaba haciendo un control masivo e indiscriminado de los datos con fines de vigilancia exterior, esto es, en lugar de considerar medidas de vigilancia individuales, lo que había eran programas de vigilancia.

---

[70] RUIZ MARTÍNEZ, E., 2020. Invalidez del Privacy Shield ¿Hay una salida? *Revista de Derecho vLex*, no. 196. PP .2-3.
[71] MORENO, V., 2020. *Viviane Reding: "El Brexit es una verdadera catástrofe para la UE, pero lo será aún más para los británicos".* 3 de febrero. Disponible en: https://www.expansion.com/juridico/actualidad-tendencias/2020/02/03/5e34593ee5fdea3a2a8b45ef.html.
[72] "He [Schrems] was actually the trigger for me to understand that we couldn't continue the way the law was applied", LEVINE, R., 2015. *Behind the european privacy ruling that's confounding Silicon Valley.* 9 de octubre. Disponible en: https://www.nytimes.com/2015/10/11/business/international/behind-the-european-privacy-ruling-thats-confounding-silicon-valley.html.
[73] Comisión Europea. 2016. La Comisión Europea pone en marcha el Escudo de la Privacidad UE-EE.UU.: más protección para los flujos de datos transatlánticos. 12 de julio. Disponible en: https://ec.europa.eu/commission/presscorner/detail/es/IP_16_2461.
[74] RUIZ MARTÍNEZ, E., 2020. Op. Cit. PP 3-4.

Al no poner límites la normativa estadounidense a la injerencia en la intimidad ni dar herramientas legales a los ciudadanos para defenderse, se vulneraba el principio de proporcionalidad y se producía una falta de garantías, lo que derivó en la Sentencia del 16 de julio de 2020 del TJUE que invalidaba el Privacy Shield.

2.2 Reino Unido y el *Brexit*

Como no podía ser de otra manera, entre el maremágnum de materias negociadas entre Reino Unido y la Unión Europea estaba la protección de datos, tema que se encuentra entre los artículos 71 y 74 del Acuerdo sobre la retirada del Reino Unido de Gran Bretaña e Irlanda del Norte de la Unión Europea y de la Comunidad Europea de la Energía Atómica de 31 de enero de 2020. Sin necesidad de extenderse mucho, en el Acuerdo se compromete el Reino Unido a seguir el nivel protección del RGPD; y la UE acuerda no tratar diferente al Reino Unido a otros Estados miembro "sólo" por dejar la Unión. Además, el Gobierno británico ya se ha comprometido a incluir el RGPD en el ordenamiento jurídico interno[75], por lo que esperamos una norma igual de proteccionista que el Reglamento.

2.3 China

El caso de China es particular. En primer lugar, no encontramos traducción oficial de la Ley de Ciberseguridad de la República Popular China, en vigor desde el 1 de junio de 2017, por lo que puede ocurrir que la versión analizada de la norma[76] y la bibliografía que trata la norma puedan tener algún error de interpretación. En segundo lugar, la propia estructura de la ley la convierte en una norma un tanto ecléctica por cuanto que trata materias que en el caso de España suelen ir por separado[77]: LOPDGDDGDD; Reglamento de la LOPDGDD; Ley de Servicios de la Sociedad de la Información; Ley General de

---

[75] "After the end of the transition period, GDPR will be retained in UK law and will continue to be read alongside the Data Protection Act 2018, with technical amendments to ensure it can function in UK law. The UK remains committed to high data protection standards", Department for Digital, Culture, Media & Sport, Department for Business, Energy & Industrial Strategy, and Information Commissioner's Office., 2020. Using personal data in your business or other organization. 31 de diciembre. Disponible en: https://www.gov.uk/guidance/using-personal-data-in-your-business-or-other-organisation-after-the-transition-period#data-protection-and-gdpr.

[76] Creemers, et al. 2018. *Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017).* 29 de junio. Disponible en: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/

[77] RAMÍREZ MORÁN, D., 2017. Ciberseguridad En China. Documento Informativo. Instituto Español De Estudios Estratégicos, no. Ramírez Morán, David., P. 3.

Telecomunicaciones; Ley de Protección de Infraestructuras Críticas; Código Civil; Código Penal; Esquema nacional de seguridad; y Esquema nacional de ciberseguridad. Se entiende que este desarrollo se corresponde a la intención de planificar un control transversal de todo lo que abarcan los sistemas de información, y no tanto tratar la seguridad de los internautas en particular[78].

Y decimos "control", no "regulación", por lo que establece el Capítulo 3: monitorización de actividad en la red y almacenamiento de los datos durante seis meses (art. 21); los equipos "críticos" y los especializados en ciberseguridad deben ser aprobados por un establecimiento autorizado antes de ser vendidos (art. 23); obligación de proporcionar la identidad real a los "*operadores de red que manejen el acceso a la red y servicios de registro de nombres de dominio para usuarios, acceso a la red de telefonía fija o móvil, o prestan a los usuarios servicios de publicación de información o mensajería instantánea*", además de fomentar la investigación y desarrollo de tecnologías para la identificación de ciudadanos e implementar una "*estrategia de credibilidad de identidad en la red*" (art. 24); obligación de los proveedores de red de prestar asistencia técnica a los organismos públicos dedicados a la salvaguardia de la seguridad nacional en la investigación de crímenes (art. 28), siendo un posible ejemplo el de la publicación de *deep fakes*[79], vídeos en los que se superpone la cara de una persona sobre otra para que parezca que ha hecho algo que no ocurrió; y todo se enmarca en el artículo 30, que indica que toda esta información sólo se puede obtener con el fin de proteger la ciberseguridad, sea lo que sea que entiendan como tal.

III. LOS DATOS PERSONALES TAMBIÉN SE "INFECTAN" DE COVID-19

1. SANIDAD

1.1 Uso de aplicaciones informáticas

1.1.1 Radar COVID

La aplicación para móviles Radar COVID tiene como propósito informar al usuario de que en los últimos catorce días ha estado en contacto con una persona infectada

[78] Íbid.
[79] Reuters Staff. 2019. *China seeks to root out fake news and deepfakes with new online content rules.* 29 de noviembre. Disponible en: https://www.reuters.com/article/us-china-technology/china-seeks-to-root-out-fake-news-and-deepfakes-with-new-online-content-rules-idUSKBN1Y30VU.

por COVID, entendiéndose por "contacto" el pasar con esa persona más de quince minutos a menos de dos metros[80] .

El desarrollo de la aplicación ha generado muchas dudas, pero ha resultado ser bastante aséptica: se descarga la app; se aceptan las condiciones de uso y la política de privacidad; y desde ese momento Radar COVID genera cada día un código identificador "pseudo-aleatorio" que se intercambia con otros móviles cercanos que hayan descargado la aplicación a través de las funciones bluetooth. La búsqueda de otros códigos se da cada cinco minutos, y los almacena de forma local -archivos propios y ajenos- por si se notificase un positivo en los próximos 14 días. Precisamente el positivo comunica como sigue: la persona afectada puede introducir en la app el "código de confirmación de un solo uso" que le proporcionará el Servicio Público de Salud, y éste se validará en el servidor. Entonces, la aplicación solicitará al usuario su consentimiento para enviar los códigos aleatorios que generó su dispositivo los últimos 14 días al servidor de la app, para así saber, con perdón de la literalidad del mecanismo, qué códigos anónimos y aleatorios han estado en contacto en los últimos 14 días con otros códigos anónimos y aleatorios de otras personas con la misma app. Una vez el sistema detecte que se dan las condiciones para un posible contagio, se le manda al posible infectado al móvil una notificación en el que se le dice que ha estado en contacto con un positivo, la fecha en que se dio, y se le invita a confinarse y ponerse en contacto con las autoridades sanitarias.

Es decir, los desarrolladores han prestado mucha atención a dos claves:

Que se garantice el anonimato de los usuarios con el uso de los códigos aleatorios, tanto para la administración como para los contactos. Sobre estos últimos, es cierto que la notificación quizá suene a *alguien ha contagiado a alguien*[81], pero es el punto intermedio entre privacidad e información que se ha encontrado.

Que se pida permiso a cada paso hacia la intromisión de la intimidad. La aplicación no trabaja, ni procesa datos, ni envía ni recibe nada sin el permiso expreso del usuario en cada situación.

---

[80] Gobierno de España. *POLÍTICA DE PRIVACIDAD DE LA APLICACIÓN Radar COVID*. Disponible en: https://radarcovid.covid19.gob.es/terms-of-service/privacy-policy.html.
[81] Miguel Gila. *Alguien ha matado a alguien.* Disponible en: https://youtu.be/gLZQpvvyeQc.

Una vez explicado el funcionamiento de la aplicación se puede apreciar que se diseñó pensando en no dejar cabos sueltos en cuanto a la protección de datos, pero la informática es muy compleja y todavía hay dudas.

1.1.1.1 El código de Schrödinger

En la física cuántica se recurre a la paradoja del gato de Schrödinger para ilustrar que el estado de un objeto es una cosa y su contraria simultáneamente, y que lo que determina el resultado es la observación. O, dicho de otro modo, no sabemos cómo suena un árbol que cae si no hay nadie alrededor para oírlo. No se sabe porque, efectivamente, falta la observación. Radar COVID no era de código abierto, a diferencia de lo que sucede con las aplicaciones de otros países, lo que abrió un debate entre informáticos[82].

Por un lado, se defendió el código abierto para que la comunidad de especialistas que están interesados pueda acceder al interior de la app y, así, perfeccionarla entre todos; por no hablar de que la aplicación se ha desarrollado con dinero público, por lo que se debería enseñar el resultado al público, valga la redundancia. Lo de la participación de la comunidad no es baladí, pues mucho software se ha creado a partir del trabajo desinteresado de gente con conocimientos, los cuales han sido volcados a programas con licencia Creative Commons[83].

Por otro lado, hay quienes no le dieron mayor importancia, bien porque consideraban que era una cuestión de tiempo que se acabase liberando, bien porque la prioridad era publicar la app lo antes posible y nadie se había preocupado por esto.

Finalmente se liberó el código[84] y, aparentemente, éste no presenta problemas para la privacidad[85], a pesar de las dudas con los dispositivos que disponen del sistema operativo Android 6 en adelante.

---

[82] MONDÉJAR ARÁEZ, D., 2020. *Radar COVID, a examen: ¿es segura la APP de rastreo del Gobierno?* 12 de agosto. Disponible en: https://www.lasexta.com/noticias/nacional/radar-covid-examen-segura-app-rastreo-gobierno_202008125f33bb4bffbf6a00012b7af7.html.

[83] *Creative Commons.* Disponible en: https://creativecommons.org/.

[84] PÉREZ, E., 2020. *Radar COVID libera su código fuente y será compatible con otras aplicaciones europeas por si viajamos fuera.* 9 de septiembre. Disponible en: https://www.xataka.com/aplicaciones/radar-covid-libera-hoy-su-codigo-fuente-sera-compatible-otras-aplicaciones-europeas-viajamos-fuera.

[85] AGUILAR, R., 2020. *Radar Covid, Análisis a fondo de su código: cómo funciona, qué está bien, qué está mal y qué falta.* 10 de septiembre, Disponible en: https://www.xatakandroid.com/analisis/radar-covid-analisis-a-fondo-su-codigo-como-funciona-que-esta-bien-que-esta-mal-que-falta.

1.1.1.2 Las API de Google, bluetooth y la geolocalización como cooperadora necesaria

Las API son "un conjunto de comandos, funciones y protocolos informáticos que permiten a los desarrolladores crear programas específicos para ciertos sistemas operativos. Las API simplifican en gran medida el trabajo de un creador de programas, ya que no tiene que «escribir» códigos desde cero. Estas permiten al informático usar funciones predefinidas para interactuar con el sistema operativo o con otro programa[86]". Es decir, las API son necesarias para el uso de varias de las herramientas del teléfono, entre ellas el bluetooth. Ahora bien, suelen requerir permisos y, en este caso, se pide poder tener acceso a la localización del dispositivo[87]:

"El otro permiso que debes declarar es ACCESS_FINE_LOCATION[88]. Tu app necesita este permiso porque es posible usar un escaneo de Bluetooth para reunir información sobre la ubicación del usuario. Esta información puede obtenerse desde el dispositivo del usuario o desde balizas Bluetooth en determinados lugares, como tiendas y áreas de tránsito."

Esto significa que Radar COVID requiere unas herramientas que necesitan poder tener acceso a la geolocalización para poder hacer uso del bluetooth, pero no quiere decir que haga uso de esa opción. O, dicho de otro modo, como decía Julio César Fernández Muñoz, desarrollador de iOS y editor de Applesfera.com[89]: "*la API de localización usa solo la de Bluetooth para el escaneo y medir la distancia entre dispositivos para saber la incidencia o no de la exposición, pero no puede geolocalizarte físicamente y la API Exposure Notification no registra dato alguno de localización. El ID que se genera aleatorio, es lo único que se transmite, junto al dato de la intensidad de la señal Bluetooth. No hay dato de localización alguno en la transmisión ni el sistema lo almacena. Y esto está auditado porque el código de Exposure Notification es abierto*".

---

[86] ABC Tecnología., 2015. *¿Qué es una API y para qué sirve?* 16 de febrero. Disponible en: https://www.abc.es/tecnologia/consultorio/20150216/abci--201502132105.html.

[87] Developers Android. *Introducción general a bluetooth.* Disponible en: https://developer.android.com/guide/topics/connectivity/bluetooth?hl=es-419

[88] "Allows an app to access precise location". Developers Android. *Access_fine_location*. Disponible en: https://developer.android.com/reference/android/Manifest.permission?hl=es-419#ACCESS_FINE_LOCATION.

[89] PASTOR, J., 2020. *Por qué Radar Covid no funciona sin el GPS activo en Android pero sí lo hace en los iPhone.* 12 de agosto. Disponible en: https://www.xataka.com/aplicaciones/que-radar-covid-no-funciona-gps-activo-android-hace-iphone.

Radar COVID tenía ante sí un reto complicado, y no cabe duda de que los desarrolladores lo han hecho lo mejor han sabido, pero no es código todo lo que reluce.

1.1.1.3 Lo que Amazon ofrece fuera de carta

Probablemente le sorprenda saber que la sombra de Amazon abarca no "sólo" el de la venta y envío de productos[90]; vídeo bajo demanda[91]; música por streaming[92]; o retransmisiones en directo[93]; también ofrece servidores[94], sólo que éste último servicio no está disponible para el público de a pie. No hablamos de servidores pequeños: Netflix, Mango, El Corte Inglés, Glovo, Booking, y medios de comunicación entre otras muchas empresas hacen uso de sus servidores[95] y servicios informáticos, incluyendo Radar COVID.

Se ha descubierto que Amazon, cuyo software se utiliza para comunicar el positivo desde Radar COVID, podía saber quién comunicaba su positivo a través de la app: los archivos que se envían no se pueden leer, pero la aplicación sólo los envía cuando se comunica el positivo en COVID[96]. De este modo, Amazon podía saber que alguien era positivo porque sabía que ese archivo sólo se envía en ese caso. Este fallo lo evitaron en otros países europeos creando un tráfico falso de información, enviándose así positivos reales y archivos sin información real, de modo que el proveedor del servicio no puede saber qué se comunica. De hecho, ahora que ya se ha informado de la corrección del error[97], la solución ha sido precisamente el envío de falsos positivos al servidor.

---

[90] *Amazon*. Disponible en: https://www.amazon.es/.
[91] *Prime Video*. Disponible en: https://www.primevideo.com/.
[92] *Amazon Music*. Disponible en: https://music.amazon.es/?ref=dm_aff_amz_es.
[93] *Twitch*. Disponible en: https://www.twitch.tv/.
[94] *Amazon Web Services*. Disponible en: https://aws.amazon.com/es/.
[95] PLAZA, A., 2018. *El hilo del que pende internet: si Amazon Web Services falla, te quedas sin estas webs*. 1 de agosto, Disponible en: https://www.elconfidencial.com/tecnologia/2018-08-01/aws-amazon-web-hilo-pende-internet-servidores_1599622/.
[96] PÉREZ COLOMÉ, J., 2020. *La 'app' Radar Covid ha tenido una brecha de seguridad desde su lanzamiento*. 22 de octubre. Disponible en: https://elpais.com/tecnologia/2020-10-22/la-app-radar-covid-ha-tenido-una-brecha-de-seguridad-desde-su-lanzamiento.html.
[97] @AppRadarCovid. 2020. *Actualización RadarCOVID*. 9 de octubre. Disponible en: https://twitter.com/AppRadarCovid/status/1314476420828192769?s=20.

1.1.2 Aplicaciones de auto-test

Cada Comunidad autónoma ha sacado su propia aplicación y/o página web para que el ciudadano pueda someterse a una autoevaluación orientativa para conocer la probabilidad de estar padeciendo la COVID-19. Cada administración autonómica trabaja en sus propios términos: en un lado tenemos casos como el de Castilla y León, donde se evita el tratamiento de datos personales[98]; y en el otro extremo está la Comunidad de Madrid, que pide al usuario su nombre completo; DNI; número de teléfono; fecha de nacimiento; dirección completa (incluyendo código postal y comunidad autónoma); género; geolocalización opcional -en el registro y en autoevaluaciones que se deben realizar cada 12 horas)-; y, finalmente, también los datos relacionados con la autoevaluación propiamente dicha -temperatura, contactos recientes con positivos, etc.-. Lo cierto es que la mayoría de la información que piden no sirven al propósito del servicio -dar resultado de la autoevaluación; dar consejos; hacer un seguimiento del progreso de los síntomas-; aunque se puede entender que responden a otros objetivos: finalidades estadísticas; investigación biomédica, científica o histórica; y para archivo en interés público[99] (es decir, lo que prevé el artículo 9 RGPD).

1.2 Rastreadores

1.2.1 Quiénes son los rastreadores

Aunque se asocien con profesionales sanitarios, en realidad no es necesario. En este sentido, Fernando Simón, director del Centro de Coordinación de Alertas y Emergencias Sanitarias, que "*los técnicos que van a hacer el seguimiento de contactos es cierto que no requieren un nivel de formación específico ni especialmente alto*"; "*si lo son mejor, pero no es necesario que los técnicos sean sanitarios. No es lo especialmente importante. Además, hay que entender estos profesionales no surgen de debajo de las piedras; los titulados son los que hay y están prácticamente todos ahora trabajando con el coronavirus*[100]". Desde la perspectiva jurídica se antoja complicado hacer la misma valoración pues no se ha creado jurisprudencia ni escrito suficientes artículos jurídicos

---

[98] Sanidad de Castilla y León. *Test COVID-19*. Disponible en: https://covidapps.saludcastillayleon.es/COVI/.

[99] Comunidad de Madrid., 2020. *Política de privacidad de la aplicación CoronaMadrid.* 7 de abril. Disponible en: https://coronavirus.comunidad.madrid/politica-de-privacidad/.

[100] GARCÍA, Y., 2020. *¿Qué son y qué hacen los rastreadores? Así vigilan El COVID-19.* 18 de julio. Disponible en: https://www.newtral.es/rastreadores-covid-19-funciones-espana/20200718/.

con los que poder valorar con garantías si los rastreadores requieren una habilitación especial.

1.2.2 Autoridad ante el ciudadano

"No somos la Guardia Civil", se lamentaba una rastreadora cuando se refería a aquellas personas que no seguían sus indicaciones[101]. "Yo les pido que se queden en casa pero hay veces que cuando vuelvo a llamar al domicilio, no hay nadie. ¿Y qué puedo hacer? Nada. […] Yo cuando les vuelvo a llamar, si no estaban, les monto un pollo y les digo que voy a mandar a la policía local a su casa. Pero es un farol, porque no puedo hacer nada", explicaba otra rastreadora[102]. Y estas declaraciones se referían a las indicaciones para guardar cuarentena, pero cabe preguntarse si los rastreadores tienen autoridad para exigir a una persona que le diga dónde, cuándo y con quién ha estado. En este último caso, al ciudadano se le pide la identificación de los contactos estrechos sin que éstos sepan que se están cediendo sus datos.

A juicio de este autor, no se está prestando suficiente atención a las implicaciones de estas preguntas, por muy necesarias que sean las medidas para frenar la expansión de la pandemia. Cuando se le pregunta a una persona dónde ha estado, quizá el precio sea revelar su orientación sexual[103]; o que le tenga explicar una infidelidad al rastreador y a su pareja[104]. Y en este contexto de confesión de intimidades, no es raro mentirle a alguien al que no reconoces autoridad alguna[105]: "*Algunos nos mienten […]. En ocasiones*

---

[101] LÓPEZ MADRID, C., 2020. *Los Rastreadores: "Llamas a un contacto aislado y está aparcando el coche".* 22 de junio. Disponible en: https://webcache.googleusercontent.com/search?q=cache:vOe07_mZMfUJ:https://www.lavanguardia.com/vida/20200622/481892570418/rastreadores-sanitarios-covid-coronavirus-espana-espana.html+&cd=1&hl=es&ct=clnk&gl=es.

[102] CASTRO, C., 2020. *Rastreadores, los detectives del coronavirus.* 19 de julio. Disponible en: https://www.elindependiente.com/vida-sana/salud/2020/07/19/rastreadores-los-detectives-del-coronavirus/.

[103] Bloomberg., 2020. *Corea choca con el estigma de la homosexualidad en plena lucha contra el coronavirus.* 11 de mayo. Disponible en: https://www.lavanguardia.com/internacional/20200511/481103799460/corea-del-sur-brote-seul-coronavirus-pubs-bares-clubes-gay.html.

[104] BARAHONA, P. y RUSO, F., 2020. *Los 'cazadores' del Covid-19: su misión, localizar al que haya estado 15 minutos con un positivo.* 30 de mayo. Disponible en: https://www.elespanol.com/reportajes/20200530/cazadores-covid-19-mision-localizar-minutos-positivo/493701681_0.html.

[105] Núñez y Alfonso., 2020. *Rastreadores de covid: así trabajan para frenar los rebrotes.* 17 de julio. Disponible en: https://www.niusdiario.es/sociedad/sanidad/rastreadores-covid-coronavirus-medicos-asi-trabajan-frenar-rebrotes_18_2979120257.html.

tenemos que insistir en que no hacemos labores policíacas. Hay gente que no reconoce que ha estado en un bar a las cinco de la mañana porque a lo mejor no se lo comunicó a su familia más directa".

La mención a la Guardia Civil resulta acertada porque corresponde a los Cuerpos y Fuerzas de Seguridad del Estado el "velar por el cumplimiento de las Leyes y disposiciones generales, ejecutando las órdenes que reciban de las Autoridades, en el ámbito de sus respectivas competencias". Es decir, la Policía y la Guardia Civil tendrían una mayor autoridad para obtener respuestas a preguntas personales.

2. COMPLIANCE

El *compliance* comprende un conjunto de medidas -evaluación de riesgos, organización y control de procesos y proyectos - encaminadas a evitar o reducir el riesgo de perpetrar conductas sancionables[106]. En el caso de la protección de datos, las empresas y demás organizaciones deben trabajar en estas medidas para procesar y almacenar correctamente los datos personales siguiendo lo establecido en el RGPD, incluso pudiendo incurrir en delito en su caso.

La Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, incluyó novedades en lo concerniente a la responsabilidad penal de las personas jurídicas que encontramos en su artículo 31 bis, y poco tiempo después la Fiscalía General del Estado publica la Circular 1/2016, de 22 de enero. En ella se dice que "*el objeto de los modelos de organización y gestión no es solo evitar la sanción penal de la empresa sino promover una verdadera cultura ética corporativa, de tal modo que su verdadera eficacia reside en la importancia que tales modelos tienen en la toma de decisiones de los dirigentes y empleados y en qué medida constituyen una verdadera expresión de su cultura de cumplimiento*". Por tanto, el *compliance* tiene una estrecha relación con la cultura de cumplimiento y compromiso con el Derecho por parte todos los miembros de la organización. No se trata de cumplir con las normas para evitar sanciones, sino por convicción, por saber de su necesidad y utilidad.

[106] AMADEO GADEA, S. y FORTUNY CENDRA, M., 2018. Una aproximación a la responsabilidad de los administradores y de las personas jurídicas. Madrid: Escoda. P. 139

Finalmente, poco más de un mes después de la Circular, el Tribunal Supremo aprecia por primera vez responsabilidad penal en personas jurídicas en su Sentencia 154/2016 de 29 de febrero de 2016. Siguiendo la línea de la Fiscalía, el Tribunal dice que *"la determinación del actuar de la persona jurídica, relevante a efectos de la afirmación de su responsabilidad penal, ha de establecerse a partir del análisis acerca de si el delito cometido por la persona física en el seno de aquélla, ha sido posible o facilitado por la ausencia de una cultura de respeto al derecho como fuente de inspiración de la actuación de su estructura organizativa e independiente de la de cada una de las personas jurídicas que la integran, que habría de manifestarse en alguna clase de formas concretas de vigilancia y control del comportamiento de sus directivos y subordinados jerárquicos tendentes a la evitación de la comisión por éstos de los delitos"*.

3. TRANSPORTE

3.1 Conservación de datos de pasajeros

La trazabilidad[107] es un medidor importante para saber si se tiene bajo control -o no- una pandemia. Es por eso por lo que se publicó el 29 de junio de 2020 una Resolución de la Dirección General de Salud Pública, Calidad e Innovación que obliga a los viajeros procedentes de fuera de España que lleguen por mar o aire a someterse a un control sanitario antes de entrar en el país: control de temperatura, documental y visual sobre el estado del pasajero. En el caso de la temperatura, el control será rutinario y no se almacenará dato o imagen relacionada con el proceso; y en cuanto al control documental, los viajeros deberán cumplimentar un formulario antes de viajar en el que deben indicar nombre, número de teléfono, información de vuelo, dirección de residencia, lugar de estancia, países visitados en los últimos catorce días, si se ha tenido contacto con una persona con COVID en ese plazo, si presenta síntomas o si ha estado en un hospital últimamente.

[107] "Proporción de casos de los que se conoce el origen". BORRAZ, M., 2020. Qué es la trazabilidad del coronavirus: el indicador clave que Sanidad propone en su nuevo semáforo para saber si hemos perdido el rastro al virus. 17 de octubre. Disponible en: https://www.eldiario.es/sociedad/trazabilidad-coronavirus-indicador-clave-sanidad-propone-nuevo-semaforo-si-hemos-perdido-rastro-virus_1_6295659.html.

3.2 Turistas y CCAA

España decidió hace tiempo que nuestra economía debía fiarlo casi todo al turismo y la hostelería, lo que ha hecho que exista un serio choque entre la economía y la salud como consecuencia de la pandemia. Intentando encontrar un punto medio, se han dado iniciativas como que los viajeros deban avisar de su llegada a la Comunidad Autónoma de destino, siendo éste el caso de Galicia[108], y dar una serie de datos personales en el proceso[109]: número de pasaporte, NIE o DNI; nombre, apellidos y territorio de procedencia; datos de contacto, es decir, número de teléfono y correo electrónico; y datos de la estancia, que incluyen fechas de llegada y salida del territorio, y lugar de estancia.

Además, los artículos 17 y 18 del Real Decreto-ley 21/2020, de 9 de junio, de medidas urgentes de prevención, contención y coordinación para hacer frente a la crisis sanitaria ocasionada por el COVID-19 obligan a las empresas de transporte de pasajeros a que conserven sus datos de contacto durante cuatro semanas cuando el vehículo disponga de número de asiento preasignado.

4. CONSUMO

4.1 Aceptando las cookies

Las cookies[110] son pequeños archivos que se almacenan en los dispositivos cuando se navega por internet y que contienen información de nuestras visitas: contraseña para acceder a nuestro espacio personal en la web; el contenido de la cesta con los productos a comprar y que adquirimos finalmente más tarde; o la configuración que hayamos elegido, como el idioma con el que interactuamos con la página. El propósito de estas cookies en particular es la de agilizar la navegación en páginas ya visitadas, y se conocen como las “cookies necesarias”.

---

[108] RESOLUCIÓN de 1 de octubre de 2020, de la Dirección General de Salud Pública, en la cual se determinan los territorios a efectos de la aplicación de la obligación de comunicación prevista en la Orden de 27 de julio de 2020 por la que se establecen medidas de prevención para hacer frente a la crisis sanitaria ocasionada por el COVID-19, en relación con la llegada a la Comunidad Autónoma de Galicia de personal procedente de otros territorios.

[109] Orden de 27 de julio de 2020 por la que se establecen medidas de prevención para hacer frente a la crisis sanitaria ocasionada por el COVID-19 en relación con la llegada a la Comunidad Autónoma de Galicia de personas procedentes de otros territorios.

[110] IONOS., 2021. *La aplicación de la ley de cookies europea en España.* 4 de marzo. Disponible en: https://www.ionos.es/digitalguide/paginas-web/derecho-digital/la-ley-de-cookies-y-su-aplicacion-en-espana/.

Más lucrativas son las "cookies no necesarias" porque son aquellas que realizan funciones que no tienen que ver con el funcionamiento de la web, sino que sirven para obtener información sobre los usuarios: gustos, edades, ubicación, perfiles de redes sociales, ideología, etc. La motivación que hay detrás de esto no es saber cómo es una persona en particular, sino recopilar ingentes cantidades de datos para formar lo conocido como *big data* y sus cuatro "V": almacenamiento de un gran Volumen de datos; procesados a gran Velocidad; que abarcan una gran Variedad de materias; y de los que se puede extraer un gran Valor[111]. El big data puede utilizarse para multitud de propósitos[112]: campañas de marketing y ventas; estimar la probabilidad de que se cometa un crimen en un lugar en particular; anticiparse a posibles lesiones en el deporte; o saber dónde encontrar a potenciales votantes. La COVID ha sido durante muchos meses el monotema, y todos hablan de ella a todas horas. Que se busque información sobre este virus puede parecer que no tiene gran importancia de cara a la privacidad porque, si es tan popular en los motores de búsqueda, no sería un dato que defina a nadie en particular, pero no es así.

Una popular serie de televisión, aun siendo consumida por las masas de todo el mundo y todas las edades, puede decir mucho de uno mismo. Se sabe que el equipo de campaña de Donald Trump se sirvió de las herramientas del big data de cara a las elecciones presidenciales de Estados Unidos en 2016 para saber, por ejemplo, que entre los cerca de 17 millones de espectadores de The Walking Dead[113] de por aquel entonces, una serie sobre un mundo post-apocalíptico infestado de muertos vivientes, había mucha preocupación sobre la inmigración; y que los de NCIS, con unas cifras parecidas[114], eran más contrarios al *ObamaCare*[115]. El big data sirve para esto, para aglutinar una abrumadora cantidad de datos diferentes y cruzarlos para obtener unos perfiles que serían imposibles de esbozar de otra forma.

---

[111] Instituto de Ingeniería del Conocimiento. *Big Data.* Disponible en: https://www.iic.uam.es/big-data/.
[112] UNIR Revista., 2020. *Ejemplos de big data en la actualidad.* 6 de febrero. Disponible en: https://www.unir.net/ingenieria/revista/ejemplos-big-data/.
[113] EFE., 2016. *"The Walking Dead" roza su mayor récord de audiencia.* 26 de octubre. Disponible en: https://www.efe.com/efe/america/cultura/the-walking-dead-roza-su-mayor-record-de-audiencia/20000009-3078038.
[114] F. DEL CASTILLO, B., 2016. *'NCIS' sube con el final de su decimotercera temporada en CBS.* 18 de mayo. Disponible en: https://www.formulatv.com/noticias/56222/audiencias-eeuu-17-de-mayo-ncis-coupled/.
[115] BERTONI, S., 2016. *Exclusive interview: how Jared Kushner won Trump the White House.* 20 de diciembre. Disponible en: https://www.forbes.com/sites/stevenbertoni/2016/11/22/exclusive-interview-how-jared-kushner-won-trump-the-white-house/#19eb07362f50.

Las cookies no necesarias pueden revelar a terceros nuestras inquietudes más íntimas, sobre todo si las búsquedas que hacemos hacen pensar que estamos infectados de la COVID-19 o de cualquier otro virus. Después, estas terceras partes procesan esta información personal y hacen negocio con él sin que, quizá, el usuario sea consciente de ello, o al menos no lo sea todo lo que debiera.

4.2 Con tarjeta o en metálico

Se venía observando desde hace tiempo que el pago con tarjeta -incluso el móvil- estaba desplazando el pago en efectivo, pero que los billetes y las monedas pasen por tantas manos hace que esta tendencia se acelere con la COVID[116]. Todos los pagos hechos con tarjeta quedan registrados. Esto significa que, así como se explicaba antes en el apartado de las cookies, las entidades bancarias saben en qué se gastan el dinero sus clientes, pero no es el único dato: también revelamos dónde estamos. En Corea del Sur, por ejemplo, existe una aplicación para vigilar la cuarentena de 14 días y, además de vigilar que llevas el móvil contigo, también observan las transacciones con tarjeta[117].

4.3 Datos personales de clientes

La trazabilidad[118] es un medidor importante para saber si se tiene bajo control -o no- una pandemia. Por este motivo, el artículo 26 del Real Decreto-ley 21/2020, de 9 de junio, de medidas urgentes de prevención, contención y coordinación para hacer frente a la crisis sanitaria ocasionada por el COVID-19 dice lo siguiente:

"Los establecimientos, medios de transporte o cualquier otro lugar, centro o entidad pública o privada en los que las autoridades sanitarias identifiquen la necesidad de realizar trazabilidad de contactos, tendrán la obligación de facilitar a las autoridades

---

[116] Bolsamanía., 2020. *¿Acabará el covid con el dinero en efectivo? Un 64% ya lo usa menos que hace un año*. 22 de septiembre. Disponible en: https://www.bolsamania.com/noticias/finanzas-personales/acabara-covid-dinero-efectivo-64-usa-menos--7649838.html.

[117] BECKER, A., 2020. *¿Exagera la aplicación alemana de rastreo de COVID-19 con la protección de datos?* 17 de diciembre. Disponible en: https://www.dw.com/es/exagera-la-aplicaci%C3%B3n-alemana-de-rastreo-de-covid-19-con-la-protecci%C3%B3n-de-datos/a-55975456.

[118] "Proporción de casos de los que se conoce el origen". BORRAZ, M., 2020. Qué es la trazabilidad del coronavirus: el indicador clave que Sanidad propone en su nuevo semáforo para saber si hemos perdido el rastro al virus. 17 de octubre. Disponible en: https://www.eldiario.es/sociedad/trazabilidad-coronavirus-indicador-clave-sanidad-propone-nuevo-semaforo-si-hemos-perdido-rastro-virus_1_6295659.html.

sanitarias la información de la que dispongan o que les sea solicitada relativa a la identificación y datos de contacto de las personas potencialmente afectadas".

En relación con este tipo de medidas, informa la AEPD[119] que los datos deben recogerse de manera proporcionada con la finalidad, no extralimitándose en la cantidad, siendo éste el principio de minimización de datos recogido en el RGPD. Esto significa que con tener número, día y hora en la que el cliente se encontraba en el establecimiento es suficiente para avisar a las personas potencialmente perjudicadas, evitando así tener que alarmar a demasiadas personas. Además, aclara la AEPD que los datos que pueden recopilar y, en su caso, facilitar los establecimientos a las autoridades no se encuentran dentro de las "categorías especiales" del RGPD, aunque el propósito sea el de controlar la pandemia.

5. OTRAS MEDIDAS

5.1 Cámaras de detección de temperatura corporal como control de accesos

Decía la AEPD[120] que las cámaras térmicas son especialmente delicadas porque, en primer lugar, estos dispositivos señalan un dato relativo a la salud de las personas como es la temperatura corporal, y se presume a partir de él que una persona está afectada por el coronavirus; y segundo, porque estos aparatos se colocan en espacios públicos y condicionan el acceso, de modo que si alguien supera una determinada temperatura y no se le deja pasar, otras personas presumirán que ese individuo padece la COVID. Además, el consentimiento no es libre pues, si no accedes a que te tomen la temperatura, no pasas.

Las cámaras tienen mejor encaje para el ámbito laboral, y es algo que se podría alegar en un centro comercial por cuanto que ahí hay personas trabajando y el empleador debe velar por la seguridad de sus empleados, pero la AEPD prefiere buscar y aplicar otras medidas menos invasivas por las razones expuestas en el primer párrafo.

---

[119] Agencia Española de Protección de Datos., 2020. *Comunicado sobre la recogida de datos personales por parte de los establecimientos.* 31 de julio. Disponible en: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-sobre-la-recogida-de-datos-personales-por-parte-de-los-establecimientos.

[120] Agencia Española de Protección de Datos., 2020. Comunicado de la AEPD en relación con la toma de temperatura por parte de comercios, centros de trabajo y otros establecimientos. 30 de abril, Disponible en: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-aepd-temperatura-establecimientos.

En cualquier caso, la buena fe y el sentido común es imprescindible por parte de los establecimientos, renunciando a ciertas fórmulas dudosas como "informar" al cliente que está dando su consentimiento para la toma de temperatura sin que éste lo supiese de antemano (ver Anexo II[121]).

5.2 La cartilla COVID

Pasando por alto la dudosa efectividad de la cartilla ante un virus cambiante[122], lo cierto es que supondría una grave vulneración del derecho a la intimidad el tener que revelar datos médicos por sistema, incluso para encontrar trabajo[123]. Se trataría a juicio de este autor de una medida inconstitucional[124] y contraria a la normativa europea, en particular al RGPD y su artículo 9 que protege especialmente los datos relativos a la salud.

IV. VALORACIÓN JURÍDICA DEL USO DE DATOS ANTE LA COVID-19

1. POSIBLES PROBLEMAS GENERALES QUE CONSIDERAR

1.1 Derecho a la intimidad vs. Interés general y derecho a la información

El derecho fundamental a la intimidad sobrevive en el conflicto, y para muestra está la lista de disputas que tiene con otros derechos en el Anexo I. Estos conflictos se pueden dirimir en favor del interés general, el cual es un concepto jurídico indeterminado de difícil definición, pero que podemos entender que se trata del consenso en cuanto a intereses comunes en una sociedad[125]; o como una cláusula abstracta que representa un bien jurídico identificado por los poderes públicos para resolver cuestiones y necesidades sociales[126]. El derecho a la intimidad se encuentra en este grupo, pero a veces pasa de ver

---

[121] Elaboración propia.
[122] Organización Mundial de la Salud., 2020. *"Immunity passports" in the context of COVID-19.* 24 de abril, Disponible en: https://www.who.int/publications/i/item/immunity-passports-in-the-context-of-covid-19.
[123] Europa Press Madrid., 2020. *Ayuso Defiende La 'cartilla Covid': "no descarto que sea necesaria para acceder a empleos".* 31 de julio. Disponible en: https://www.lavanguardia.com/local/madrid/20200731/482589087556/ayuso-cartilla-vovid-acceder-empleos.html.
[124] Art. 18.1 CE.
[125] MONTALVO ALBIOL, J.C., 2011. Interés General y administración contemporánea. Revista de filosofía, derecho y política, Universitas, no. 14., P. 140.
[126] ACOSTA GALLO, P., 2019. Interés general. Eunomía. Revista en cultura de la legalidad., no. 16. P. 180.

los demás derechos "al lado" a tenerlos enfrente. En particular, con quien más fricciones tiene el derecho a la intimidad es con el derecho a la información.

Sin ánimo de reproducir las noticias por congruencia con el discurso propio, en los meses anteriores se han visto publicaciones que decían cosas como "*Dos familias de un bloque de viviendas de la calle [nombre calle] de [municipio] han dado positivo por coronavirus, por lo que el Ayuntamiento, […] ha decretado el confinamiento de todo el edificio hasta que a los vecinos se les hagan las pruebas PCR*", acompañado de una foto que tenía al pie "*El bloque de viviendas afectado en [municipio]*"[127]; o en una pieza sobre otro confinamiento en otro bloque[128]: "*Tan profundo respiró [nombre]al salir este miércoles del portal del barrio de [nombre del barrio] que deformó la mascarilla*"; seguido en el mismo texto de "*cuando Salud Pública ordenó el confinamiento de los 97 vecinos del bloque [número] de [calle] el pasado día 27 de junio*"; más fotos del portal.

No se discute la relevancia e interés público de informar sobre la cuarentena en un bloque de viviendas -siendo éste un requisito para hacer prevalecer el derecho a la información sobre la intimidad[129]-, sino si toda la información que la acompaña, como la dirección, imágenes del edificio con vecinos saliendo del portal -cuando pueden-, o incluso un vídeo en el que se ve a una vecina de uno de estas viviendas saliendo al encuentro con la ambulancia que le llevaría al hospital[130] es necesaria para dar la noticia[131]. El artículo 7.5 de la LO 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen considera ilegítima la "*la captación, reproducción o publicación por fotografía, filme, o cualquier otro*

---

[127] Naiz., 2020. *Confinan un bloque de viviendas En Hernani tras detectarse varios positivos entre sus residentes.* 28 de julio, Disponible en: https://www.naiz.eus/eu/info/noticia/20200728/confinan-un-bloque-de-viviendas-en-hernani-tras-detectarse-varios-positivos.

[128] ROJO, J.C., 2020. *Sanidad desconfina a los 83 vecinos De Castilla-Hermida que dan negativo en los test: «Ya estamos libres»*. 8 de julio, Disponible en: https://www.eldiariomontanes.es/santander/autorizan-salir-mayor-20200708125459-nt.html?ref=https:%2F%2Fwww.google.com%2F.

[129] "Ello significa que para indagar si en un caso concreto el derecho de información debe prevalecer será preciso y necesario constatar, con carácter previo, la relevancia pública de la información, ya sea por el carácter público de la persona a la que se refiere o por el hecho en sí en que esa persona se haya visto involucrada, y la veracidad de los hechos y afirmaciones contenidos en esa información"; SENTENCIA 171/1990, de 12 de noviembre, FJ 5.

[130] RIVAS, I., 2020. *Brote de Santander: 30 nuevos aislados relacionados con el edificio en cuarentena.* 29 de junio. Disponible en: https://www.niusdiario.es/sociedad/coronavirus-santander-aislados-relacionados-edificio-cuarentena_18_2970720185.html.

[131] "El criterio para determinar la legitimidad o ilegitimidad de las intromisiones en la intimidad de las personas no es el de veracidad, sino exclusivamente el de la relevancia pública del hecho divulgado, es decir, que su comunicación a la opinión pública, aun siendo verdadera, resulte necesaria en función del interés público del asunto sobre el que se informa", STC 172/1990, de 12 de noviembre; FJ 3

procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos, salvo los casos previstos en el artículo octavo, dos", es decir, "*la información gráfica sobre un suceso o acaecimiento público cuando la imagen de una persona determinada aparezca como meramente accesoria*", considerándose como imagen accesoria una toma general de un espacio público donde aparezca un conjunto de personas[132].

En lo concerniente a las fotografías de personas fallecidas[133] y el derecho a la protección de datos, el RGPD no se les aplica[134], y lo que prevé la LOPDGDD concierne a las facultades que se otorgan a sus familiares en cuanto a datos, pero a los fallecidos no se les reconoce el derecho a la intimidad.

1.2 La inmunidad en el currículum

Unas páginas atrás comentábamos que la cartilla COVID suponía una injerencia en el derecho a la intimidad, el cual es un derecho negativo. Ahora bien, uno puede hacer uso de su derecho a la protección de datos -derecho activo- y hacer público en su currículum o entrevista de trabajo que ha superado la COVID. Por un lado, y desde la perspectiva del aspirante, uno puede revelar la información que crea oportuna si lo decide libremente; por otro lado, esta situación pone en un compromiso al empleador pues si éste decide quedárselo y no obtiene el permiso expreso del entrevistado para procesar esa información, entonces no le queda más remedio que destruir el documento[135].

1.3 *Social login* y circulación de datos de infectados

Es común ver en páginas web que se nos da la oportunidad de iniciar sesión con una cuenta de Google, Facebook, Twitter, Instagram; lo que nos facilita el proceso de registro ahorrándonos escribir nombre, correo electrónico, pensar -y recordar- una nueva contraseña, etc. Esta forma de registro e inicio de sesión se denomina social login, y a

---

[132] MACIÁ-BARBER, C., 2020. COVID-19 En portada: radiografía ética de la cobertura fotográfica de la pandemia en España. Revista Española en Comunicación en Salud, no. Suplemento 1, S42-S58. P. 44.
[133] Íbid, PP. 53-54.
[134] Párrafos 27, 158 y 160 de los puntos considerados.
[135] ESTEBAN, P., 2020. *Incluir La inmunidad al covid en el currículum es legal, pero pone al empresario en apuros.* 28 de mayo. Disponible en: https://cincodias.elpais.com/cincodias/2020/05/27/legal/1590608875_092681.html.

cambio de la comodidad se abre un camino de dos carriles: la empresa cuya cuenta se usa -Facebook, LinkedIn, etc.- sabe en qué otras páginas te registras; y el propietario de esa página -por ejemplo, unos grandes almacenes- tiene acceso a la actividad del contacto en esa red social y recopilar información personal de ahí[136]. Esto significa que la información íntima que el usuario revela está a disposición de la red en que la publica, sus seguidores y también para el vendedor o prestador de servicios donde se ha registrado. Se trata, por tanto, de información especialmente protegida que circula y se mueve mucho más lejos de lo que el usuario cree.

1.4 "No somos la Guardia Civil"

La recuperación de esta cita no tiene sólo el propósito de rescatar un tema anterior, que también, sino que además resulta útil para sintetizar en una frase el quid de la cuestión: no se cuestiona en ningún momento la utilidad o necesidad de los rastreadores, sino su legitimidad legal para irrumpir en la intimidad de las personas.

1.4.1 Rastreadores ante el espejo: la seguridad privada.

Aquella frase pronunciada por una rastreadora la podría haber dicho un guardia de seguridad privada, y por eso se le toma de ejemplo para desarrollar el argumento de quien escribe.

Visualicemos la siguiente escena: usted acude a un establecimiento comercial para adquirir uno o varios productos. Cuando se dispone a salir con su bolsa por la puerta, el arco de seguridad suena con fuerza. Usted, que ha pagado por lo que se está llevando e imagina que el problema está en una alarma no retirada, probablemente le entregue la bolsa y el tique de compra al guardia para que lo revise para probar que todo es fruto de un malentendido.

Ahora imaginemos la misma escena, pero usted, que no es un ladrón y le ofende que otros piensen que lo sea, avergonzado además por ser objeto de atención del resto de

---

[136] RODRÍGUEZ, P., 2020. *Hay empresas que tiene extensos informes con tus datos personales recopilados en internet y los venden por más cien euros.* 16 de abril. Disponible en: https://www.xataka.com/privacidad/hay-empresas-que-tiene-extensos-informes-tus-datos-personales-recopilados-internet-venden-cien-euros.

clientes, se niega a enseñarle nada. Usted ha pagado, no tiene que demostrar nada a nadie y se dispone a salir -no antes sin presentar la hoja de reclamaciones-. El guardia, que tiene unas obligaciones[137], no le piensa dejar marchar, así que en virtud de sus competencias le retiene y avisa a la Policía para que proceda a realizar el registro correspondiente[138], pues se trata de una acción que interfiere con el derecho fundamental a la intimidad del art. 18.1 CE, estando los guardias no sólo no habilitados para realizarlo, sino que además lo tienen prohibido[139].

1.4.2 La Ley Orgánica como herramienta esencial

No hay discrepancias con la Agencia Española de Protección de Datos cuando dicen que el RGPD no debe ser un obstáculo en la lucha contra la pandemia en su informe N/REF: 0036/2020, pero los derechos fundamentales a la intimidad y la protección de datos no están suspendidos, y el RGPD prevé la posibilidad de las injerencias en favor del interés general, aunque no de cualquier manera. Antes de "invadir" la intimidad de alguien, se deben establecer "*medidas adecuadas y específicas para proteger los derechos y libertades del interesado*" [140].; y en relación con el caso que nos ocupa; el artículo 81 CE explica que son las leyes orgánicas las que desarrollan los derechos fundamentales y libertades públicas.

2. LEY ORGÁNICA 3/1986, DE 14 DE ABRIL, DE MEDIDAS ESPECIALES EN MATERIA DE SALUD PÚBLICA

[137] Art. 32 Ley 5/2014 de 4 de abril, de Seguridad Privada.
[138] Art. 32.1.d) bis
[139] Sentencia de la Audiencia Provincial de Barcelona 254/2015, 18 de marzo, 2015, FJ1.
[140] Art. 9.2.i) RGPD: "El tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional".

2.1 Desarrollo

Las Comunidades Autónomas han publicado una serie de Decretos que establecen un régimen sancionador, como los de Murcia[141] o la Comunidad Valenciana[142]. No todas las Administraciones mencionan la Ley Orgánica que encabeza este apartado, pero ésta resulta esencial. Se trata de una norma muy corta de cuatro artículos.

Como su título sugiere, tiene el propósito de otorgar a las autoridades sanitarias de las distintas Administraciones Públicas[143] amplios poderes para actuar en situaciones excepcionales en los que se ponga en peligro la salud pública. Así, "*podrán adoptar medidas de reconocimiento, tratamiento, hospitalización o control cuando se aprecien indicios racionales que permitan suponer la existencia de peligro para la salud de la población*"[144]; y además[145]:

"Con el fin de controlar las enfermedades transmisibles, la autoridad sanitaria, además de realizar las acciones preventivas generales, podrá adoptar las medidas oportunas para el control de los enfermos, de las personas que estén o hayan estado en contacto con los mismos y del medio ambiente inmediato, así como las que se consideren necesarias en caso de riesgo de carácter transmisible".

Finalmente, el cuarto artículo, que se modificó hace apenas unos meses mediante Decreto-Ley[146], prevé la posibilidad de establecer medidas en caso de desabastecimiento de medicamentos y productos sanitarios.

2.2 A favor

[141] Decreto-Ley n.º 8/2020, de 16 de julio, por el que se establece el régimen sancionador por el incumplimiento de las medidas de prevención y contención aplicables en la Región de Murcia para afrontar la situación de crisis sanitaria ocasionada por el Covid-19.
[142] DECRETO LEY 11/2020, de 24 de julio, del Consell, de régimen sancionador específico contra los incumplimientos de las disposiciones reguladoras de les medidas de prevención ante la Covid-19.
[143] Artículo 1.
[144] Artículo 2.
[145] Artículo 3.
[146] Real Decreto-ley 6/2020, de 10 de marzo, de 10 de marzo, por el que se adoptan determinadas medidas urgentes en el ámbito económico y para la protección de la salud pública.

Hay una serie de razones por las que sus defensores entienden que es una norma bien desarrollada[147], y que se proceden a sintetizar en las próximas líneas. En primer lugar, se afirma que la LO es "un precepto legal cristalinamente claro" porque, en efecto, el literal de la norma permite tomar las medidas que crean necesarias para controlar el riesgo de una enfermedad transmisible sin límite. En segundo lugar se dice que, aunque la competencia para regular derechos fundamentales la tenga el Estado mediante ley orgánica, ésta no incluye la de ejecución, por lo que cualquier administración puede restringir derechos fundamentales si la ley le habilita para ello, como sería el caso del tercer artículo. El tercer argumento a favor es que el hecho de que el Estado tenga la competencia para declarar el estado de Alarma, Excepción y Sitio y adoptar medidas en base a éstos, no impide que las comunidades autónomas tomen medidas similares por su cuenta, pues el art. 116 CE no lo impide, y tampoco la LO que desarrolla el artículo; y que en caso de conflicto entre aquella y la LO de Medidas Especiales en Salud Pública debería prevalecer la segunda por ser más actual.

También se defiende que la norma sea tan abierta porque las condiciones y garantías de la limitación de derechos se pueden encontrar en el resto del ordenamiento jurídico; porque la medida requiere ratificación judicial[148]; y porque el TC admitió en su Sentencia 69/1989 que las normas limitativas de derechos fundamentales pueden tener en sus textos conceptos jurídicos indeterminados.

2.3 Dudas en su aplicación

Quien escribe estas líneas no puede evitar tener la sensación de que el visto bueno de los defensores de la LO corresponde más a sus deseos que a un análisis honesto de la norma.

Cuando se discute la indeterminación de la LO no es porque no sea clara, que lo es por cuanto queda claro que no pone límites, sino porque precisamente ese es su fallo: necesitamos conocer los límites de la norma para tener garantías. Esto ya lo tratamos al

---

[147] DOMENECH, G., 2020. *Comunidades Autónomas, derechos fundamentales y Covid-19*. 21 de julio. Disponible en: https://almacendederecho.org/comunidades-autonomas-derechos-fundamentales-y-covid-19#comments.

[148] Art. 8-6 LRJCA

principio del presente Trabajo con el caso Malone[149]; y el TC ya declaró inconstitucional un precepto de la LO de Régimen Electoral General que limitaba el derecho a la protección de datos por no especificar el interés público que limitaba el derecho; por no precisar las restricciones posibles y por no dar las garantías adecuadas[150].

Estamos hablando de una LO que se está entendiendo como una vía para las CCAA para disponer de plenos poderes de una manera totalmente arbitraria. Hay expresiones en el tercer artículo como "podrá adoptar las medidas oportunas"; y "así como las que se consideren necesarias" que crean inseguridad jurídica. Impedir a una persona salir de casa o hacerle confesar intimidades no forma parte de las competencias de una Comunidad Autónoma -ni siquiera en el ámbito penal se le puede obligar a nadie a declararse culpable[151]-. Quizá habría que preguntarse por qué existe esta LO si en su artículo primero se dice que las medidas se podrán tomar "dentro del ámbito de sus competencias" pues, si no pueden ir más allá de sus competencias, entonces no se sabe qué aporta esta norma.

3. PROPUESTA

Resumen el nudo gordiano en el que se ha convertido el rastreo de contactos: tenemos a una persona infectada, se le pregunta con quién ha estado, dónde y cuándo en las dos últimas semanas; y éste puede no acceder a dar esta información. Este método presenta varios obstáculos: el rastreador no tiene autoridad para exigir esos datos -otra cosa es que el individuo acepte responder, ahí no hay problema-, de modo que dependemos de la voluntad de alguien que no sabemos cómo reaccionará con el sobresalto del positivo.

Lo que se va a exponer a continuación es una humilde propuesta relativa a la búsqueda de contactos a través de rastreadores.

---

[149] La injerencia en las comunicaciones debe estar "prevista en la ley", que debe ser asequible para el ciudadano y expresada con la suficiente precisión como para que exista seguridad jurídica.
[150] Sentencia del Tribunal Constitucional 76/2019, de 22 de mayo, fundamentos jurídicos 7 y 8.
[151] Art. 118.1.h) LECrim

3.1 Los rastreadores como "nueva" autoridad pública: posible artículo 556.3 del Código Penal

Para reforzar la autoridad de los rastreadores se plantea la posibilidad de considerar a los rastreadores como autoridad pública. Es cierto que el artículo 550 CP ya considera a los funcionarios sanitarios como autoridades públicas, pero hay que hacer dos incisos:

- La condición de autoridad es sólo para funcionarios. Ahora bien, el artículo 556.1 CP incluye a la seguridad privada "que desarrolle actividades de seguridad privada en cooperación y bajo el mando de las Fuerzas y Cuerpos de Seguridad".
- Los rastreadores no necesariamente tienen por qué ser sanitarios ni funcionarios, como ya se ha indicado anteriormente, que es lo que ya sucede con los agentes de seguridad privada.

Se trata, por tanto, de recoger expresamente la figura del rastreador como autoridad en el Código Penal, o al menos encajarla como la seguridad privada, y aprovechar lo estipulado en el artículo 556.1 CP incorporando un nuevo punto 3 que quedaría aproximadamente como sigue:

"*Serán castigados […] los que, sin estar comprendidos en el artículo 550, resistieren o desobedecieren gravemente a las instrucciones de los rastreadores sanitarios, debidamente identificados, en el ejercicio de sus funciones de control y trazabilidad de enfermedades transmisibles, que desarrollen actividades de comunicación de resultados médicos a las personas afectadas, seguimiento de casos confirmados, y trazado de contactos de las personas afectadas por la infección con el propósito de evitar su propagación. Estas funciones se desempeñarán siempre bajo el mando de las Autoridades Sanitarias y en colaboración con las Fuerzas y Cuerpos de Seguridad, de acuerdo con la cooperación interadministrativa y deber de colaboración prevista en la legislación, de modo que la escasa gravedad penal de la desobediencia no será óbice para que pueda incurrir en infracción administrativa.*

Todos los datos personales obtenidos y procesados por los rastreadores en el ejercicio de sus funciones se tratarán de acuerdo con lo previsto en la normativa europea y española vigente".

Se han destacado los elementos clave del artículo. En primer lugar, lógicamente, se delimita la infracción: no seguir las instrucciones de los rastreadores en el desarrollo

de sus funciones. En segundo lugar, se legitima la autoridad y protección de los rastreadores al encontrarse bajo el paraguas de las autoridades sanitarias -ya lo están, pero se refuerza esa jerarquía al mencionarlo expresamente, no hablamos de los rastreadores como intrusos que se infiltran en el Código Penal-. En tercer lugar, la mención a las Fuerzas y Cuerpos de Seguridad, la cooperación y colaboración interadministrativa, y la mención a las sanciones administrativas se refieren a la Ley de Seguridad Ciudadana y sus artículos 7 y 8. Si bien esta norma no prevé infracciones penales, sí las prevé administrativas, y puede funcionar como una forma de sanción subsidiaria. La Ley prevé como criterio para graduar la gravedad de la sanción el "*riesgo producido para la seguridad ciudadana o la salud pública*". Finalmente, se cierra el artículo mencionando de soslayo el actual RGPD y la LOPDGDD. En particular, esa frase apunta al artículo 9 RGPD, apartados g)[152] e i)[153].

Esta novedad normativa le daría a los rastreadores la autoridad necesaria para, al menos, no ser menospreciados por los ciudadanos; incluso permitiría actuar frente a personas que no guardan cuarenta habiendo dado positivo por considerar que ponen en riesgo la salud pública.

La empresa no es pequeña pues supone actualizar una Ley Orgánica, sobre todo considerando la prisa que tendría la entrada en vigor del precepto, pero el poder legislativo ha demostrado que, si quiere, se puede[154].

VI. CONCLUSIONES

1. En la regulación que se ha ido construyendo hasta el presente se observan dos velocidades: por un lado, tenemos convenios en los que se sientan las bases del derecho a la intimidad y privacidad que han permanecido estables con los años, como ocurre con los hechos en Roma en 1950 y Estrasburgo de 1981; por otro, aquellas normas que entraban en el detalle de estos derechos han terminado por quedar obsoletas. El motivo es que el avance de la tecnología ha hecho necesario

[152] "El tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado".

[153] "El tratamiento es necesario por razones de interés público en el ámbito de la salud pública".

[154] RICO, J., 2018. *Así se reforma la Constitución en dos meses.* 17 de septiembre. Disponible en: https://www.elperiodico.com/es/politica/20180917/proceso-reforma-constitucion-expres-7038522.

dotar de más herramientas a los usuarios, y de obligaciones a quienes tratan datos personales.

2. Actualmente el ciudadano tiene más conocimiento sobre la protección de datos, y qué consecuencias e implicaciones tienen sus actos públicos y, sobre todo, en internet. Se ha hecho mucho hincapié en los derechos de acceso, rectificación, supresión y oposición; y también se ha hecho un esfuerzo por mejorar la transparencia en relación con el uso que se hace de los datos personales cuando se visita una página web o se descarga una aplicación para el móvil. Sin embargo, estos avances son más pronunciados en lugares como la Unión Europea, pero no tanto en otros como Estados Unidos, y a pesar de los intentos por compatibilizar las regulaciones de unos y otros -Safe Harbour y Privacy Shield-, ninguno de estos acuerdos ha prosperado.

3. La llegada de la pandemia del coronavirus ha agudizado los conflictos de la protección de datos y el derecho a la intimidad ante otros derechos, como el de la vida, información y libre circulación de personas. Existe una lógica urgencia por parar el crecimiento del virus y paliar sus consecuencias, y para eso se necesitan datos: quién, dónde, cuándo, cuánto. Esta información la necesitan las Administraciones, sí, pero también los ciudadanos y los medios de comunicación, así como la mayoría de los sectores económicos y, en particular, aquellos que dependen del turismo y los viajes en general. Quedan por delante muchos meses -o años- en los que la protección de datos deberá adaptarse a la nueva normalidad, como todos nosotros.

VII. BIBLIOGRAFÍA

Agencia de los Derechos Fundamentales de la Unión Europea; Consejo de Europa; Tribunal Europeo de Derechos Humanos; Buttarelli, G. 2018. *Manual De Legislación Europea En Materia De Protección De Datos.*

AGUILAR, R., 2020. *Radar COVID, análisis a fondo de su código: cómo funciona, qué está bien, qué está mal y qué falta.* 10 de septiembre. Disponible en: https://www.xatakandroid.com/analisis/radar-COVID-analisis-a-fondo-su-codigo-como-funciona-que-esta-bien-que-esta-mal-que-falta.

AMADEO GADEA, S. (Coordinador). y FORTUNY CENDRA, M., 2018. Una aproximación a la responsabilidad de los administradores y de las personas jurídicas. Madrid: Escoda.

BARAHONA, P. y RUSO, F., 2020. *Los 'cazadores' del COVID-19: su misión, localizar al que haya estado 15 minutos con un positivo.* 30 de mayo. Disponible en: https://www.elespanol.com/reportajes/20200530/cazadores-COVID-19-mision-localizar-minutos-positivo/493701681_0.html.

CASTILLA DEL PINO, C., 1989. Público, privado, íntimo. In: De la intimidad. Crítica. *Público, privado, íntimo*.

CASTRO-RIAL GARRONE, F., 1987. Decisiones de la Comisión y del Tribunal Europeos de Derechos Humanos. *Revista de Instituciones Europeas*, no. 15.

GARCÍA-PERROTE ESCARTÍN, I. y MERCADER UGUINA, J.R., 2017. El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril relativo al tratamiento de datos personales, un primer acercamiento. *Revista de información laboral*, no. 2/2017.

GARRIGA DOMÍNGUEZ, A., 2000. La nueva Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos personales, ¿un cambio de filosofía? *Anales de la Cátedra Francisco Suárez*, vol. 34.

MAYOR GÓMEZ, R., 2016. Contenido y novedades del Reglamento General de Protección de Datos de la UE (Reglamento UE 2016/679, de 27 de abril de 2016). *Revista del Gabinete Jurídico de la Junta De Comunidades de Castilla-La Mancha*, no. 6.

MERINO MARTÍN, J., 2019. Los datos personales relativos a la salud y la historia clínica. *Revista Aranzadi Doctrinal*, no. 10/2019.

ORTEGA GIMÉNEZ, A., 2009. Transferencia internacional de datos de carácter personal: UE Vs. EE.UU. *Revista de Derecho vLex*, no. 67.

RAMÍREZ MORÁN, D., 2017. Ciberseguridad en China. *Documento informativo. Instituto Español de Estudios Estratégicos*, no. Ramírez Morán, David.

REBOLLO DELGADO, L. y SALTOR, C.E., 2015. El derecho a la protección de datos en España y Argentina: orígenes y regulación vigente. Madrid: Dykinson.

RODRÍGUEZ DÍAZ, B.(., RAMOS DE MOLINS, A. y SANZ GANDASEGUI, F., 2015. Manual de ámbito jurisdiccional comunitario e internacional. Guía práctica para abogados ante la UE y el TEDH. Dykinson.

RUIZ MARTÍNEZ, E., 2020. Invalidez del Privacy Shield ¿Hay una salida? *Revista de Derecho vLex*, no. 196.

SUAREZ RUBIO, S.M., 2011. El derecho a la privacidad en el ámbito de la salud: Estados Unidos. Facultad de Ciencias Sociales de Cuenca.

VIII. LEGISLACIÓN

Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos)

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

Convenio 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981

Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América (Acuerdo Safe Harbour)

Decisión de Ejecución (UE) 2016/1250 de la Comisión de 12 de julio de 2016 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuaciñon de la protección conferida por el Escudo de la privacidad UE-EE.UU (Acuerdo Privacy Shield).

Declaración Americana de Derechos y Deberes del Hombre, aprobada en la Novena Conferencia Internacional Americana Bogotá, Colombia, 1948

Ley Orgánica 3/1986, de 14 de abril, de medidas especiales en materia de salud pública

Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.

Ley 5/2014, de 4 de abril, de Seguridad Privada.

Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal.

Real Decreto-Ley 6/2020, de 10 de marzo, de 10 de marzo, por el que se adoptan determinadas medidas urgentes en el ámbito económico y para la protección de la salud pública.

Decreto-Ley n.º 8/2020, de 16 de julio, por el que se establece el régimen sancionador por el incumplimiento de las medidas de prevención y contención aplicables en la Región de Murcia para afrontar la situación de crisis sanitaria ocasionada por el COVID-19.

Decreto-Ley 11/2020, de 24 de julio, del Consell, de régimen sancionador específico contra los incumplimientos de las disposiciones reguladoras de les medidas de prevención ante la COVID-19.

RESOLUCIÓN de 1 de octubre de 2020, de la Dirección General de Salud Pública, en la cual se determinan los territorios a efectos de la aplicación de la obligación de comunicación prevista en la Orden de 27 de julio de 2020 por la que se establecen medidas de prevención para hacer frente a la crisis sanitaria ocasionada por el COVID-19, en

relación con la llegada a la Comunidad Autónoma de Galicia de personal procedente de otros territorios.

Orden de 27 de julio de 2020 por la que se establecen medidas de prevención para hacer frente a la crisis sanitaria ocasionada por el COVID-19 en relación con la llegada a la Comunidad Autónoma de Galicia de personas procedentes de otros territorios.

IX. JURISPRUDENCIA

Attorney General v. Edison Telephone Company, QueenŽs Bench Division, volumen 6, 1880

Caso de Malone v. Reino Unido (Sentencia 8691/79), de 2 de agosto de 1984

Caso de Leander v. Suecia (Sentencia 9248/81), de 26 de marzo de 1987

Caso de I v. Finlandia (Sentencia 20511/03), de 17 de julio de 2008

Sentencia del Tribunal Constitucional 73/1982, de 2 de diciembre

Sentencia del Tribunal Constitucional 76/2019, de 22 de mayo

Sentencia de la Audiencia Provincial de Barcelona 254/2015, 18 de marzo

X. PÁGINAS WEB

Amazon. Disponible en: https://www.amazon.es/.

Amazon Music. Disponible en: https://music.amazon.es/?ref=dm_aff_amz_es.

Amazon Web Services. Disponible en: https://aws.amazon.com/es/.

Chart of Signatures and Ratifications of Treaty 223. Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. 29 de marzo de 2021. Disponible en: *https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures*.

Creative Commons. Disponible en: https://creativecommons.org/.

Prime Video. Disponible en: https://www.primevideo.com/.

Twitch. Disponible en: https://www.twitch.tv/.

@AppRadarCOVID., 2020. *Actualización RadarCOVID.* 9 de octubre. Disponible en: https://twitter.com/AppRadarCOVID/status/1314476420828192769?s=20.

ABC Tecnología., 2015. *¿Qué es una API y para qué sirve?* 16 de febrero. Disponible en: https://www.abc.es/tecnologia/consultorio/20150216/abci--201502132105.html.

Agencia Española de Protección de Datos., 2020a. Comunicado De La AEPD En relación con la toma de temperatura por parte de comercios, centros de trabajo y otros establecimientos. 30 de abril. Disponible en: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-aepd-temperatura-establecimientos.

Agencia Española de Protección de Datos., 2020b. *Comunicado sobre la recogida de datos personales por parte de los establecimientos.* 31 de julio. Disponible en: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-sobre-la-recogida-de-datos-personales-por-parte-de-los-establecimientos.

BECKER, A., 2020. *¿Exagera la aplicación alemana de rastreo de COVID-19 con la protección de datos?* 17 de diciembre. Disponible en: https://www.dw.com/es/exagera-la-aplicaci%C3%B3n-alemana-de-rastreo-de-COVID-19-con-la-protecci%C3%B3n-de-datos/a-55975456.

BERTONI, S., 2016. *Exclusive interview: how Jared Kushner won Trump the White House.* 20 de diciembre. Disponible en: https://www.forbes.com/sites/stevenbertoni/2016/11/22/exclusive-interview-how-jared-kushner-won-trump-the-white-house/#19eb07362f50.

Bloomberg., 2020. *Corea choca con el estigma de la homosexualidad en plena lucha contra el coronavirus.* 11 de mayo. Disponible en: https://www.lavanguardia.com/internacional/20200511/481103799460/corea-del-sur-brote-seul-coronavirus-pubs-bares-clubes-gay.html.

Bolsamanía., 2020. *¿Acabará el COVID con el dinero en efectivo? Un 64% ya lo usa menos que hace un año.* 22 de septiembre. Disponible en: https://www.bolsamania.com/noticias/finanzas-personales/acabara-COVID-dinero-efectivo-64-usa-menos--7649838.html.

BORRAZ, M., 2020. Qué es la trazabilidad del coronavirus: el indicador clave que Sanidad propone en su nuevo semáforo para saber si hemos perdido el rastro al virus. 17 de octubre. Disponible en: https://www.eldiario.es/sociedad/trazabilidad-coronavirus-

indicador-clave-sanidad-propone-nuevo-semaforo-si-hemos-perdido-rastro-virus_1_6295659.html.

CASTRO, C., 2020. *Rastreadores, los detectives del coronavirus.* 19 de julio. Disponible en: https://www.elindependiente.com/vida-sana/salud/2020/07/19/rastreadores-los-detectives-del-coronavirus/.

Comunidad de Madrid., 2020. *Política de privacidad de la aplicación CoronaMadrid.* 7 de abril. Disponible en: https://coronavirus.comunidad.madrid/politica-de-privacidad/.

Creemers, et al., 2018. *Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017).* 29 de junio. Disponible en: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

Department for Digital, Culture, Media & Sport, Department for Business, Energy & Industrial Strategy, and Information Commissioner's Office., 2020. *Using personal data in your business or other organisation* . 31 de diciembre. Disponible en: https://www.gov.uk/guidance/using-personal-data-in-your-business-or-other-organisation-after-the-transition-period#data-protection-and-gdpr.

Developers Android., a. *Access_fine_location.* Disponible en: https://developer.android.com/reference/android/Manifest.permission?hl=es-419#ACCESS_FINE_LOCATION.

Developers Android., b. *Introducción general a bluetooth.* Disponible en: https://developer.android.com/guide/topics/connectivity/bluetooth?hl=es-419.

EFE., 2016. *"The Walking Dead" roza su mayor récord de audiencia.* 26 de octubre. Disponible en: https://www.efe.com/efe/america/cultura/the-walking-dead-roza-su-mayor-record-de-audiencia/20000009-3078038.

Europa Press Madrid., 2020. *Ayuso defiende la 'cartilla COVID': "No descarto que sea necesaria para acceder a empleos".* 31 de julio. Disponible en: https://www.lavanguardia.com/local/madrid/20200731/482589087556/ayuso-cartilla-vovid-acceder-empleos.html.

F. DEL CASTILLO, B., 2016. *'NCIS' Sube con el final de su decimotercera temporada en CBS.* 18 de mayo. Disponible

en: https://www.formulatv.com/noticias/56222/audiencias-eeuu-17-de-mayo-ncis-coupled/.

GARCÍA, Y., 2020. *¿Qué son y qué hacen los rastreadores? Así vigilan el COVID-19.* 18 de julio. Disponible en: https://www.newtral.es/rastreadores-COVID-19-funciones-espana/20200718/.

Gobierno de España. *Política de privacidad de la aplicación Radar COVID.* Disponible en: https://radarCOVID.COVID19.gob.es/terms-of-service/privacy-policy.html.

Instituto de Ingeniería del Conocimiento. *Big Data.* Disponible en: https://www.iic.uam.es/big-data/.

IONOS., 2021. *La aplicación de la ley de cookies europea en España.* 4 de marzo. Disponible en: https://www.ionos.es/digitalguide/paginas-web/derecho-digital/la-ley-de-cookies-y-su-aplicacion-en-espana/.

LÓPEZ MADRID, C., 2020. *Los rastreadores: "llamas a un contacto aislado y está aparcando el coche".* 22 de junio. Disponible en: https://webcache.googleusercontent.com/search?q=cache:vOe07_mZMfUJ:https://www.lavanguardia.com/vida/20200622/481892570418/rastreadores-sanitarios-COVID-coronavirus-espana-espana.html+&cd=1&hl=es&ct=clnk&gl=es.

MARZOCCHI, O., 2020. *La protección de los datos personales.* Diciembre. Disponible en: https://www.europarl.europa.eu/factsheets/es/sheet/157/la-proteccion-de-los-datos-personales#:~:text=El%20Convenio%20n.,de%20la%20protecci%C3%B3n%20de%20datos.

Miguel Gila. *Alguien ha matado a alguien.* Disponible en: https://youtu.be/gLZQpvvyeQc.

MONDÉJAR ARÁEZ, D., 2020. *Radar COVID, a examen: ¿es segura la APP de rastreo del Gobierno?* 12 de agosto. Disponible en: https://www.lasexta.com/noticias/nacional/radar-COVID-examen-segura-app-rastreo-gobierno_202008125f33bb4bffbf6a00012b7af7.html.

Núñez y Alfonso., 2020. *Rastreadores de COVID: así trabajan para frenar los rebrotes.* 17 de julio. Disponible en: https://www.niusdiario.es/sociedad/sanidad/rastreadores-COVID-coronavirus-medicos-asi-trabajan-frenar-rebrotes_18_2979120257.html.

Organización Mundial de la Salud., 2020. *"Immunity passports" in the context of COVID-19.* 24 de abril. Disponible en: https://www.who.int/publications/i/item/immunity-passports-in-the-context-of-COVID-19.

PASTOR, J., 2020. *Por qué Radar COVID no funciona sin el GPS activo en Android pero sí lo hace en los iPhone.* 12 de agosto. Disponible en: https://www.xataka.com/aplicaciones/que-radar-COVID-no-funciona-gps-activo-android-hace-iphone.

PÉREZ COLOMÉ, J., 2020. *La 'app' Radar COVID ha tenido una brecha de seguridad desde su lanzamiento.* 22 de octubre. Disponible en: https://elpais.com/tecnologia/2020-10-22/la-app-radar-COVID-ha-tenido-una-brecha-de-seguridad-desde-su-lanzamiento.html.

PÉREZ, E., 2020. *Radar COVID libera su código fuente y será compatible con otras aplicaciones europeas por si viajamos fuera*. 9 de septiembre. Disponible en: https://www.xataka.com/aplicaciones/radar-COVID-libera-hoy-su-codigo-fuente-sera-compatible-otras-aplicaciones-europeas-viajamos-fuera.

PLAZA, A., 2018. *El hilo del que pende internet: si Amazon Web Services falla, te quedas sin estas webs.* 1 de agosto. Disponible en: https://www.elconfidencial.com/tecnologia/2018-08-01/aws-amazon-web-hilo-pende-internet-servidores_1599622/.

Reuters Staff., 2019. *China seeks to root out fake news and deepfakes with new online content rules.* 29 de noviembre. Disponible en: https://www.reuters.com/article/us-china-technology/china-seeks-to-root-out-fake-news-and-deepfakes-with-new-online-content-rules-idUSKBN1Y30VU.

RUBAL THOMSEN, M., 2018. *Internet en China: acceso limitado.* 14 de febrero. Disponible en: https://www.lavanguardia.com/vida/junior-report/20180213/44754795638/internet-china-acceso-limitado-censura-escudo-dorado-gran-cortafuegos.html.

Sanidad de Castilla y León. *Test COVID-19.* Disponible en: https://COVIDapps.saludcastillayleon.es/COVI/.

UNIR Revista., 2020. *Ejemplos de Big Data en la actualidad*. 6 de febrero. Disponible en: https://www.unir.net/ingenieria/revista/ejemplos-big-data/.

XI. ANEXOS

1. ANEXO 1

		En relación con el respeto a:			
		Vida privada y familiar		Domicilio y correspondencia	
Derechos (nº artículo)	**Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales**	**Ejemplos**	**Sentencias TEDH**	**Ejemplos**	**Sentencias TEDH**
	Vida (2)	Exhumación en una investigación criminal, respeto a la memoria de la familia.	Caso de Solska y Rybicka v. Polonia (Sentencias nº 30491/17 and 31083/17).	Posición activa de la administración para proteger las viviendas de posibles inundaciones.	Caso de Kolyadenko y otros v. Rusia (Sentencias nº 17423/05, 20534/05, 20678/05, 23263/05, 24283/05 y 35673/05).
	Prohibición de la tortura (3)	Desnudar y registrar personas.	Caso de Wainwright v. Reino Unido (Sentencia nº 12350/04).		
	Juicio justo (6)	Comunicación confidencial entre cliente y abogado en prisión.	Caso de Altay v. Turquía (Sentencia nº 11236/09).		
	Libertad de pensamiento, de conciencia y religiosa (9)	Obligación de revelar creencias religiosas.	Caso de Folgerø y otros v. Noruega (Sentencia nº 15472/02).		
	Libertad de expresión (10)	Difamación sobre personaje público y familiares.	Caso de Tamiz v. Reino Unido (Sentencia nº 3877/14).	Protección de fuentes periodísticas.	Caso de Telegraaf Media Nederland Landelijke Media y otros v. Países Bajos (Sentencia nº 39315/06).

	Derecho a un recurso efectivo (13)			Notificar al interesado del fin de las medidas de vigilancia e interceptación de comunicaciones para poder; así como proporcionar infomación para que se pueda impugnar posteriormente.	Caso de Roman Zakharov v. Rusia (Sentencia nº 47143/06).
	Prohibición de discriminación (14)	Ataque y destruccion de casas de ciudadanos romaníes.	Caso de Burlya v. Ucrania (Sentencia nº 3289/10).	La herencia del derecho al arrendamiento se aplica también a parejas del mismo sexo.	Caso de Karner v. Austria (Sentencia nº 40016/98).
	Demandas individuales (34)			Interceptación de cartas del TEDH al actor por terceros.	Caso de Yefimenko v. Rusia (Sentencia nº 152/04).
	Protocolos adicionales al Convenio	**Ejemplos**	**Sentencias TEDH**	**Ejemplos**	**Sentencias TEDH**
	Protección de la propiedad (Protocolo nº1, art. 1)			Imposibilidad de volver al domicilio familiar por ocupación militar.	Caso de Chiragov y otros v. Armenia (Sentencia nº 13216/05).
	Libertad de circulación (Protocolo Nº4, art. 2)			Personas que viven en una caravana debajo de una carretera, con altos niveles de contaminación.	Caso de Ward v. Reino Unido (Sentencia nº 31888/03).

2. ANEXO II


PLENILUNIO
SHOPPING CENTER
POR TU SEGURIDAD, ESTAMOS
MIDIENDO LA TEMPERATURA CORPORAL
DE MANERA VOLUNTARIA
GRACIAS POR TU DISPOSICIÓN Y COMPRENSIÓN
AQUÍ, TU SEGURIDAD ES LO PRIMERO
PROTECCIÓN DE DATOS
El afectado queda informado de los siguientes aspectos:
- Fin del Tratamiento: Control de temperatura para el acceso a las instalaciones.
- Legitimación del Tratamiento: Cumplimiento de una misión de interés público en el ámbito de la salud pública.
- Conservación de los datos: Los datos no son almacenados al tratarse de una medición en tiempo real.
- Más información: Puntos de información al cliente, vía postal a PLENILUNIO SOCIMI, S.A.,
CC PLENILUNIO, S.L. Calle Aracne s/n, Pol. Empresarial Las Mercedes, 28022, Madrid o vía correo electrónico a
GDPR.Espana@klepierre.com.